Torsion Points on Elliptic curves

by

Darlison Nyirenda

Thesis presented in partial fulfilment of the requirements for the degree of Master of Science in Mathematics in the Faculty of Science at Stellenbosch University

Department of Mathematical Sciences,
University of Stellenbosch,
Private Bag X1, Matieland 7602, South Africa.

Supervisor: Dr. A. Keet

March 2013

Declaration

By submitting this thesis electronically, I declare that the entirety of the work contained therein is my own, original work, that I am the sole author thereof (save to the extent explicitly otherwise stated), that reproduction and publication thereof by Stellenbosch University will not infringe any third party rights and that I have not previously in its entirety or in part submitted it for obtaining any qualification.

Date: 2013/02/25 .....

Abstract

Torsion Points on Elliptic curves

D. Nyirenda

Department of Mathematical Sciences,

University of Stellenbosch,

Private Bag X1, Matieland 7602, South Africa.

Thesis: MSc

March 2013

The central objective of our study focuses on torsion points on elliptic curves. The case of elliptic curves over finite fields is explored up to giving explicit formulae for the cardinality of the set of points on such curves. For finitely generated fields of characteristic zero, a presentation and discussion of some known results is made. Some applications of elliptic curves are provided. In one particular case of applications, we implement an integer factorization algorithm in a computer algebra system SAGE based on Lenstra's elliptic curve factorisation method.

Opsomming

Torsiepunte op elliptiese krommes

("Torsion Points on Elliptic Curves")

D. Nyirenda

Departement Wiskunde,

Universiteit van Stellenbosch,

Privaatsak X1, Matieland 7602, Suid Afrika.

Tesis: MSc

Maart 2013

Die hoofdoel van ons studie is torsiepunte op elliptiese krommes. Ons ondersoek die geval van elliptiese krommes oor 'n eindige liggaam met die doel om eksplisiete formules vir die aantal punte op sulke krommes te gee. Vir 'n eindig-voortgebringde liggaam met karakteristiek nul bespreek ons sekere bekende resultate. Sommige toepassings van elliptiese krommes word gegee. In een van hierdie toepassings implementeer ons 'n heeltallige faktoriseringalgoritme in die rekenaar-algebrastelsel SAGE gebaseer op Lenstra se elliptiese krommefaktoriseeringmetode.

Acknowledgements

I would like to express my sincere gratitude to my surpervisor Dr. Anold Keet for his guidance and direction. Apart from supervisory task, he introduced me to related areas of mathematics that have been used as tools in this thesis. To that, words alone are not enough to express my gratitude. I am grateful to Professor Florian Breuer and Professor Stephan Wagner for introducing me to Number Theory and thus my interest to pursue studies on the subject. I want to thank the African Institute for Mathematical Sciences and Stellenbosch University for the scholarship that has seen me complete a masters' degree in Mathematics. To Professor Edward Schaefer (Santa Clara University, USA), Professor John Ryan and Dr. Khumbo Kumwenda (Mzuzu University, Malawi), I want to say a big thank you for realising potential in me and fighting tirelessly to let me pursue further studies at postgraduate level. To my classmates Tovohery Hajatiana Randrianarisoa, Evans Doe Ocansey and Frances Odumodu, thank you for social and spiritual support not forgetting the comfortable environment you set for me. You were true brothers and sister in a family. To the rest of friends, I say be blessed.

Dedications

To my brothers Roosevelt and Vitumbiko, my sisters Tiwonge and Vynida

To my dad Joel and mum Magret

Contents

Nomeclature

Symbols	**Definitions**
$\mathbb{Z}$	the set of integers
$\mathbb{R}$	the set of real numbers
$\mathbb{Q}$	the set of rational numbers
$\mathbb{C}$	the set of complex numbers
$\#G$ or $\lvert G\rvert$	the cardinality of G
(x_{ij})	a matrix with the entry x_{ij} in i^{th} row and j^{th} column
$\det(x_{ij})$	the determinant of a matrix (x_{ij})
$\bar{K}$	the algebraic closure of K
$\mathrm{Gal}(L/K)$	the Galois group of the field L over the field K
$\mathrm{GL}_n(R)$	the set of $n \times n$ invertible matrices whose entries belong to the ring R
$\lfloor x \rfloor$	the greatest integer less than or equal to x
$(G : H)$	the index of a subgroup H in a group G
$\mathrm{char}\, K$	the characteristic of a field K
$R^{\times}$	the set of units in R
$\mathrm{Quot}\, R$	the fraction field of an integral domain R

Chapter 1

Introduction

The study of polynomial systems of equations has had remarkable advancement. Of particular class is that of Diophantine equations which are equations of the form

$$f(x_1, x_2, \ldots, x_n) = 0 \quad \text{where} \quad f \in \mathbb{Q}[x_1, x_2, \ldots, x_n].$$

Some of the questions that may be asked include, but are not limited to, does $f = 0$ have solutions in $\mathbb{Q}$? If it has solutions, are they finitely many? Instead of seeking solutions in rational numbers, we may go further by looking at solutions in the algebraic closure $\bar{\mathbb{Q}}$. There is so much theory in this area and of special attention are cubic curves. A certain class of cubic curves called elliptic curves is the focal point of our study. As it will be shown, there is a natural group law on the curves which can be described geometrically. The method, called chord-tangent method is used to add points on the curves, thus giving rise to new points. So we can enumerate as many points as possible. Since elliptic curves are algebraic, there is an extensive use of algebraic geometry tools to arrive at certain results. The second and third chapters are devoted to some fundamental theory of elliptic curves. We review some relevant algebraic geometry on affine and projective varieties without going too far afield. Our focus is on the useful results that apply to algebraic curves, especially on divisors of curves. In chapter two, the group law is discussed. Unlike proving the associativity property of the addition law using explicit equations, we use the theory of divisors and isogenies for the proof. The Weil pairing is introduced and discussed since it is an important tool that is used in deducing some results concerning elliptic curves defined over finite fields. It is also applicable in some

cases for elliptic curves over $\mathbb{Q}$. Its properties are proved. The ring of isogenies called the endomorphism ring of an elliptic curve is characterized in the same chapter. We present by proof all possibilities the endomorphism ring can occur. In such a situation, we notice that the characteristic of a field imposes a further restriction on the nature of the ring. The endomorphism ring plays a role in determination of some known torsion bounds for elliptic curves. Chapter four is entirely devoted to elliptic curves defined over $\mathbb{C}$. The goal of this chapter is to show that a torus is the same as an elliptic curve. More precisely, if we start with a torus, we can construct an elliptic curve which is the 'same' as the torus. Conversely, if we start with an elliptic curve, we can construct a torus which is the 'same' as the elliptic curve we started with. This result allows us to infer the torsion structure of points on any given elliptic curve over $\mathbb{C}$ whose order divide some fixed integer. In chapter five, we present a proof of Nagell-Lutz theorem using formal groups, an approach that avoids complicated heavy calculations that involve moving the infinite point to a finite point and examining the new curve. Reduction of elliptic curves is discussed in line with formal groups and local fields. In particular, we obtain a lot of information about the torsion subgroup of an elliptic curve over $\mathbb{Q}$ using reduction modulo different primes. This information tells us about the possible size of the torsion subgroup and together with Nagell-Lutz theorem, the group becomes manageable to determine. This is backed by several examples that we provide. Chapter six looks at bounds on torsion points. We give several examples verifying the theoretical results and discuss a torsion bound due to Breuer [1]. In chapter seven, we give two applications of elliptic curves; integer factorization and cryptographic key exchange. The subject of elliptic curves is very broad. Some theorems are stated without proof and their results used.

Chapter 2

Preliminaries

The references used in this chapter are [8] and [2].

2.1 Affine and projective varieties

We look at algebraic sets in affine and projective spaces and then narrow down to algebraic curves over an arbitrary field. Unless otherwise stated, a field is assumed to be perfect and shall be denoted by K.

Definition 2.1.1. Affine n-space over K, denoted $\mathbb{A}^n$ is the set of n-tuples in which components are elements of $\bar{K}$, i.e, $\{(x_1, x_2, \ldots, x_n) : x_i \in \bar{K}\}$. The notation $\mathbb{A}^n(K)$ is used for the set of all points in $\mathbb{A}^n$ with components in K.

Definition 2.1.2. The set V is said to be an affine algebraic set if there exist polynomials $f_1, f_2, \ldots f_m$ such that $V = \{P \in \mathbb{A}^n : f(P) = 0 \text{ for } 1 \leq i \leq m\}$. The polynomials f_i for $i \in \{1, 2, \ldots, m\}$ are called defining polynomials of V. The vanishing ideal of V is the set $I(V) = \{f \in \bar{K}[X] : f(P) = 0 \ \forall \ P \in V\}$

We place a topology on $\mathbb{A}^n$ in which closed sets are precisely the algebraic sets. This topology is known as Zariski topology. We write V/K if $I(V)$ can be generated by elements of $K[X]$ and say that V is defined over K. Clearly, if defining polynomials of V have coefficients in K, then V is defined over K. Note that for any ideal $I \subset \bar{K}[X]$, we always have a finite number of generators since $\bar{K}[X]$ is Noetherian. An affine algebraic

set V is said to be an affine variety if $I(V)$ is a prime ideal of $\bar{K}[X]$, i.e $\bar{K}[X]/I(V)$ is an integral domain.

Given an affine variety V defined over K, we define its coordinate ring to be the set $K[V] := K[X]/I(V)$. In this case, for $f, g \in \bar{K}[X]$, it follows that $f = g \in K[V]$ if and only if $f - g \in I(V)$. The function field of V, denoted by $K(V)$ is quotient field of $K[V]$.

Definition 2.1.3. Let V be an affine variety. The dimension of V, denoted by $\dim(V)$ is the transcendence degree of $\bar{K}(V)$ over $\bar{K}$.

Example 2.1.4. Consider the set $V = \{(a, b)\}$. Clearly $I(V) = \langle x - a, y - b\rangle$. So $\bar{K}[V] = \frac{\bar{K}[x,y]}{\langle x-a, y-b\rangle} = \bar{K} \Rightarrow \bar{K}(V) = \bar{K}$. Hence $\dim(V) = 0$.

Let V/K be an affine variety and consider $\mathcal{M} = \{g \in K[V] : g(P) = 0\}$. Then $\mathcal{M}$ is a maximal ideal of $K[V]$ since the map $\psi : K[V] \to K$ defined as $g \mapsto g(P)$ is a ring epimorphism. We can thus localize $K[V]$ at its maximal ideal. Denote this localization by $\mathcal{O}_P(V)$. Then, we have that

$$\mathcal{O}_P(V) = \left\{ \frac{f}{g} : f, g \in K[V], g(P) \neq 0 \right\}.$$

We call $\mathcal{O}_P(V)$ the local ring of $K[V]$ at P. A function $\psi \in K(V)$ is *regular* or *defined* at $P \in V$ if $\psi = \frac{f}{g}$ for some $f, g \in K[V]$ and $g(P) \neq 0$. A point at which ψ is not defined is a pole of ψ. For a point P, observe that $\mathcal{O}_P(V) = \{\psi \in K(V) : \psi \text{ regular at } P\}$.

Those functions that are regular everywhere on V are precisely $K[V]$. Elements of $K[V]$ can be viewed as regular (polynomial) maps from V to $\bar{K} \cong \mathbb{A}^1$. The definition of a regular map can be extended to affine varieties in $\mathbb{A}^n$ for arbitrary n. Similarly, we can define a rational map between affine varieties. We will not discuss this here, so for more information, refer to [8].

Define a relation $\sim$ on $\mathbb{A}^{n+1} \setminus \{(0, 0, \ldots, 0)\}$ by $(x_0, x_1, \ldots, x_n) \sim (y_0, y_1, \ldots, y_n)$ if and only if there exists $\lambda \in \bar{K}^\times$ such that $y_i = \lambda x_i$ for all $1 \leq i \leq n$. Then $\sim$ is an equivalence relation. We call the set

$$\mathbb{P}^n := (\mathbb{A}^n \setminus \{(0, 0, \ldots, 0)\})/\sim$$

the projective n-space, and denote its elements by $[x_0 : x_1 : \ldots : x_n]$. Consider

$$U_i = \{(x_0 : x_1 : \ldots : x_{i-1} : x_i : x_{i+1} : \ldots : x_n) \in \mathbb{P}^n : x_i \neq 0\}.$$

We can scale down the coordinates by dividing each component by x_i so that elements of U_i are of the form $\left(\frac{x_0}{x_i} : \frac{x_1}{x_i} : \ldots : \frac{x_{i-1}}{x_i} : 1 : \frac{x_{i+1}}{x_i} : \ldots : \frac{x_n}{x_i}\right)$. It is easy to see that $\mathbb{A}^n \cong U_i$ up to regular isomorphism. Consider the map $\zeta_i : \mathbb{A}^n \to \mathbb{P}^n$ defined by

$$(x_1, x_1, \ldots, x_n) \mapsto (x_1 : x_2 : \ldots : x_{i-1} : 1 : x_{i+1} : \ldots : x_n).$$

We have $\zeta_i(\mathbb{A}^n) = U_i$. On the other hand, the inverse $\zeta_i^{-1} : U_i \to \mathbb{A}_i^n$ is realized as

$$(x_0 : x_1 : \ldots : x_{i-1} : x_i : x_{i+1} : \ldots : x_n) \mapsto \left(\frac{x_0}{x_i}, \frac{x_1}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i}\right).$$

Thus, we can embed $\mathbb{A}^n$ in $\mathbb{P}^n$. So $\mathbb{A}^n \subset \mathbb{P}^n$ means that the identification of $\mathbb{A}^n$ via some ζ_i is assumed. Similarly, any affine variety $V \subset \mathbb{A}^n$ can be embedded in $\mathbb{P}^n$ via the above map. The smallest closed set containing the image of V is called the projective closure of V and is denoted by $\overline{V}$. Given defining polynomials of V, we can find defining polynomials of $\overline{V}$ by homogenizing and the reverse process by dehomogenizing the polynomials.
For instance, let $f \in K[x, y, z]$ be the defining polynomial of V. Choose the embedding $x = \frac{X}{Z}$. Then $f^\star = Z^{\deg f} f(\frac{X}{Z}, \frac{Y}{Z})$ is the defining polynomial for $\bar{V}$.
We can define a projective variety and its coordinate ring of a projective variety in the same way as done for affine varieties. However, a distinction should be noted that vanishing ideals of projective varieties are homogeneous.

Definition 2.1.5. Let V be a projective variety. Choose $\mathbb{A}^n \subset \mathbb{P}^n$ with $V \cap \mathbb{A}^n \neq \emptyset$. Then the function field of V is defined as

$$\bar{K}(V) := \bar{K}(V \cap \mathbb{A}^n).$$

Thus $\bar{K}(V)$ consists of functions of the form $\frac{f}{g}$ where f and g are homogeneous of the same degree and $g \notin I(V)$. Furthermore, $\frac{f}{g} = \frac{s}{t}$ in $\bar{K}(V)$ if $ft - gs \in I(V)$. If V is defined over K, then $K(V)$ is defined in a similar manner. We call V a curve if it has dimension 1.

Definition 2.1.6. Let V be a variety with $I(V) = \langle f_1, f_2, \ldots, f_m \rangle$. A point $P \in V$ is non-singular (smooth) if the $m \times n$ matrix

$$\left(\frac{\partial f_i}{\partial x_j}(P) \right)_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$$

has rank n - $\dim(V)$. If all $P \in V$ are smooth, V is said to be smooth. Otherwise, V is singular.

If V is a curve and $P \in V$ smooth, then $\mathcal{O}_P(V)$ is a discrete valuation ring [8]. Recall that its unique maximal ideal is $\mathcal{M} = \{f \in \bar{K}[V] : f(P) = 0\}$. We define a map $\mathrm{ord}_P : \mathcal{O}_P(V) \to \mathbb{Z} \cup \{\infty\}$ by $\mathrm{ord}_P(f) = \max\{r : f \in \mathcal{M}^r\}$ which canonically extends to $\bar{K}(V)$ via $\mathrm{ord}_P(f^{-1}) = -\mathrm{ord}_P(f)$. By convention, $\mathrm{ord}_P(0) = \infty$. A uniformizer for V at P is a function $t \in K(V)$ such that $\mathrm{ord}_P(f) = 1$. Note that any $f \in K(V)$ is such that $f = ut^{\mathrm{ord}_P(f)}$ where $u \in \mathcal{O}_P(V)^\times$, and t a uniformizer at P. Thus the order of f at P is $\mathrm{ord}_P(f)$. If $\mathrm{ord}_P(f) \geq 0$, f is regular at P. Otherwise it has a pole.

Proposition 2.1.7. Let C be a curve defined over K and t a uniformizer at a smooth point $P \in C$. Then $K(C)/K(t)$ is a finite separable extension.

Proof. Since t is transcendental over K, the transcendence degree of $K(t)$ over K is 1. We also know that $K(C)$ has transcendence degree 1. Hence $K(C)/K(t)$ is a finite extension. We need to show that every $y \in K(C)$ is separable over $K(t)$. Clearly, y is algebraic over $K(t)$ so that y is a root of some polynomial $\sum_{ij} g_i(t)Y^j$ where $g_i(t) \in K(t)$. We can multiply every $g_i(t)$ by some suitable polynomial in $K[t]$ to clear out the denominators and get a relation

$$\sum_{ij} a_{ij} t^i y^j = 0.$$

Let $f(t, Y) = \sum_{i,j} a_{ij} t^i Y^j$ be the minimal polynomial of y over $K(t)$. Let $p = \mathrm{char}\ K > 0$. If f has a non-zero term $a_{ij}t^iY^j$ such that $j \neq pk$ for some integer $k \in \mathbb{Z}$, then $\frac{\partial f}{\partial Y} \neq 0$ so that y is separable over $K(t)$. Otherwise, $f(t, Y) = g(t, Y^p)$. Since K is perfect, every polynomial $h(t, Y)$ is such that $h(t^p, Y^p) = \tilde{h}(t, Y)^p$ for some $\tilde{h}(t, Y) \in K[t, Y]$. We can rearrange powers of t in $g(t, Y^p)$ so that

$$g(t, Y^p) = \sum_{l=0}^{p-1} \left(\sum_{ij} c_{ijl} t^{pi} Y^{pj} \right) t^l = \sum_{l=0}^{p-1} g_l(t, Y)^p t^l.$$

Now $\mathrm{ord}_P(g_l(t,y)^p t^l) = p\mathrm{ord}_P(g_l(t,y)) + l \equiv l \pmod{p}$. This shows that $g_l(t,y)^p t^l$'s have distinct orders at P. Recall that $f(t,y) = 0$ which yields

$$\sum_{l=0}^{p-1} g_l(t,y)^p t^l = 0. \tag{2.1.1}$$

Assume that for some $0 \leq k \leq p-1$, $g_k(t,y)^p t^k \neq 0$. Then from Equation 2.1.1, we have

$$g_k(t,y)^p t^k = -\sum_{\substack{l=0 \\ l\neq k}}^{p-1} g_l(t,y)^p t^l$$

which implies that $\mathrm{ord}_P(g_k(t,y)^p t^k) = \min\{\mathrm{ord}_P(g_l(t,y)^p t^l : l = \{0,1,\ldots,p-1\} \setminus \{k\}\}$. But this contradicts the fact that orders are distinct. So we must have $g_l(t,y)^p t^l = 0 \Rightarrow g_l(t,y) = 0$ for all $l = 0,1,\ldots,p-1$. At least one of the $g_l(t,Y)^p$'s, say $g_c(t,Y)$ must involve Y. So y is a root of $g_c(t,Y)$. However, deg $g_c(t,Y) <$ deg $f(t,Y)$, gives a contradiction to the minimality of $f(t,Y)$. □

2.2 Maps between projective curves

From now onwards, all varieties under discussion are assumed projective.

Definition 2.2.1. Let $V \subset \mathbb{P}^n$ and $W \subset \mathbb{P}^m$. A rational map from V to W is a map $\psi = [\psi_1, \psi_2, \ldots, \psi_m]$ with $\psi_i \in \bar{K}(V)$ for all $1 \leq i \leq m$, and at all points $P \in V$ where ψ_i's are regular, $\psi(P) \in W$.

The set $V(K)$ is clearly $\mathrm{Gal}(\bar{K}/K)$-invariant. We say that ψ is defined over K if $\psi^\sigma = \psi$, $\forall\, \sigma \in \mathrm{Gal}(\bar{K}/K)$, with the usual formula $\psi(P)^\sigma = \psi^\sigma(P^\sigma)$.

Definition 2.2.2. A rational map in Definition 2.2.1 is regular at P if there exists $f \in \bar{K}(V)$ such that $f\psi_i$ is regular at P for all i, and $f\psi_j(P) \neq 0$ for some j. If that happens, we set $\psi(P) = [f\psi_1(P), f\psi_2(P), \ldots, f\psi_m(P)]$. An everywhere regular rational map is called a *morphism*.

Two varieties V and W are said to be isomorphic if there exist morphisms $f : V \to W$ and $g : W \to V$ such that $f \circ g$ and $g \circ f$ are identity maps on W and V, respectively. In this case, we write $V \cong W$.

Proposition 2.2.3. Let $V \subset \mathbb{P}^n$ be a variety and C be a curve with a smooth point P. Let $\psi : C \to V$ be a rational map. Then ψ is regular at P.

Proof. We can write $\psi = [\psi_1, \psi_2, \ldots, \psi_n]$ with $\psi_i \in \bar{K}(C)$. Let t be a uniformizer at P. Set $m = \min\{r : r = \mathrm{ord}_P(\psi_i), 1 \leq i \leq n\}$. So $m = \mathrm{ord}_P(\psi_j)$ for some j. Then $\mathrm{ord}_P(t^{-m}\psi_i) \geq 0 \Rightarrow t^{-m}\psi_i$ is regular at P for all i. Also note that $\mathrm{ord}_P(t^{-m}\psi_j) = 0 \Rightarrow (t^{-m}\psi_j)(P) \neq 0$. This shows that ψ is regular at P. □

Proposition 2.2.4. Let $\psi : C_1 \to C_2$ be a morphism between curves. Then ψ is either constant or surjective.

Proof. See [8]. □

For a surjective rational map $\psi : C_1/K \to C_2/K$ which is defined over K, the map $\psi^* : K(C_2) \to K(C_1)$ given by $\psi^*(f) = f \circ \psi$ is injective. We have a tower of fields $K \subset \psi^*K(C_2) \subset K(C_1)$. Since $K(C_1)$ and $K(C_2)$ are finitely generated over K with transcendence degree 1 and using the fact that transcendence degree is additive across a tower, it follows that $[K(C_1) : \psi^*K(C_2)] < \infty$. We call ψ a *finite map*.

Definition 2.2.5. A non-constant morphism $\psi : C_1 \to C_2$ between curves is called separable, inseparable or purely inseparable if the extension $K(C_1)/\psi^*K(C_2)$ has the property in concern. We use $\deg_s\psi$ to denote the separable degree and $\deg_i\psi$ for the inseparable degree. In all cases, we have $\deg\psi = \deg_s\psi \cdot \deg_i\psi$. We also have that ψ is separable if and only if $\deg_i\psi = 1$.

Definition 2.2.6. Let $\psi : C_1 \to C_2$ be a non-constant morphism of smooth curves. For a point $P \in C_1$, let t be a uniformizer of C_2 at $\psi(P)$. We call the number

$$e_\psi(P) := \mathrm{ord}_P(t \circ \psi)$$

the ramification index of ψ at P. If $e_\psi(P) > 1$, ψ is said to be ramified at P, otherwise it is unramified at P. We say that ψ is unramified if it is unramified at all points.

We remark that the ramification index is independent of the choice of the uniformizer. Say, if t' is another uniformizer at $\psi(P)$, then $\frac{t'}{t}$ is regular and not zero at $\psi(P)$. We deduce that $\mathrm{ord}_P(t' \circ \psi) = \mathrm{ord}_P\left(t\frac{t'}{t} \circ \psi\right) = \mathrm{ord}_P(t \circ \psi) + \mathrm{ord}_P\left(\frac{t'}{t} \circ \psi\right) = \mathrm{ord}_P(t \circ \psi)$.

Proposition 2.2.7. Let $\psi : C_1 \to C_2$ be a non-constant morphism of smooth curves defined over K. Then for any $\phi \in K(C_2)$ and $P \in C_1$, we have $\mathrm{ord}_P(\phi \circ \psi) = e_\psi(P)\mathrm{ord}_{\psi(P)}(\phi)$. Furthermore, if $\beta : C_2 \to C_3$ is another non-constant morphism between curves, then $e_{\beta\circ\psi}(P) = e_\psi(P)e_\beta(\psi(P))$.

Proof. For the first part, let t be a uniformizer at $\psi(P)$. Then $\phi = t^r u$ where u is regular and not zero at $\psi(P)$. Since ψ is regular at P, we must have $u \circ \psi$ regular and not zero at $P \Rightarrow \mathrm{ord}_P(u \circ \psi) = 0$. Clearly, $\mathrm{ord}_P(\phi \circ \psi) = \mathrm{ord}_P(t^r \circ \psi) + \mathrm{ord}_P(u \circ \psi) = re_\psi(P)$. For the second part, let t' be a uniformizer at $(\beta \circ \psi)(P)$. Then $e_{\beta\circ\psi}(P) = \mathrm{ord}_P((t' \circ \beta) \circ \psi) = e_\psi(P)\mathrm{ord}_{\psi(P)}(t' \circ \beta) = e_\psi(P)e_\beta(\psi(P))\mathrm{ord}_{(\beta\circ\psi)(P)}(t') = e_\psi(P)e_\beta(\psi(P))$. □

Proposition 2.2.8. Let $\psi : C_1 \to C_2$ be a non-constant rational map between two smooth curves. Then for almost all $Q \in C_2, |\psi^{-1}(Q)| = \deg_s(\psi)$ and for any $Q \in C_2$, we have

$$\sum_{P\in\psi^{-1}(Q)} e_\psi(P) = \deg(\psi).$$

Proof. Refer to [8]. □

By Proposition 2.2.8, it is easy to show that ψ is unramified if and only if $|\psi^{-1}(Q)| = \deg(\psi)$ for all $Q \in C_2$.

2.3 Riemann-Roch Theorem and curve genus

Let C be a curve. A divisor on C is a formal finite sum D given by

$$D = \sum_{P\in C} n_P(P) \text{ where } n_P = 0 \text{ for almost all } P \in C.$$

We denote by $\mathrm{Div}(C)$ the free abelian group of divisors on C. The degree of D is the sum $\sum_{P\in C} n_P$, which we denote by $\deg D$. The divisors of degree zero form a subgroup. We use the notation $\mathrm{Div}^0(C)$ for the degree zero divisor group. We say that D is defined over K if $D^\sigma = D$ for all $\sigma \in \mathrm{Gal}(\bar{K}/K)$. We define the divisor of $f \in \bar{K}(C)$ as $\mathrm{div}(f) := \sum_{P\in C} \mathrm{ord}_P(f)(P)$. D is said to be *principal* if there exists $f \in \bar{K}(C)^\times$ such that $D = \mathrm{div}(f)$. Since $\sum_P \mathrm{ord}_P(f) = 0$, the divisors of functions form a subgroup of $\mathrm{Div}^0(C)$, and the group shall be denoted by $\mathrm{Prin}(C)$. The divisors D_1 and D_2 are said

to be linearly equivalent, written $D_1 \sim D_2$, if and only if $D_1 - D_2$ is principal. Clearly $\sim$ is an equivalence relation and we set $\mathrm{Cl}(C) := \mathrm{Div}(C)/\mathrm{Prin}(C)$ and call the quotient the *divisor class group*.

Definition 2.3.1. The *degree-0 part of the divisor class group of* C is defined to be the quotient $\mathrm{Cl}^0(C) := \mathrm{Div}^0(C)/\mathrm{Prin}(C)$. The notation $\mathrm{Div}_K(C)$ is used to emphasize elements of $\mathrm{Div}(C)$ that are invariant under the action of $\mathrm{Gal}(\bar{K}/K)$. The groups $\mathrm{Div}^0_K(C)$ and $\mathrm{Cl}^0_K(C)$ are defined in a similar way.

Proposition 2.3.2. Let $f \in \bar{K}(C)^\times$. Then $\mathrm{div}(f) = 0$ if and only if $f \in \bar{K}^\times$. Furthermore, $\deg(\mathrm{div}(f)) = 0$.

Proof. Suppose $f \in \bar{K}$. Then f has no poles (or zeros) on C so that $\mathrm{ord}_P(f) = 0$ for all $P \in C$. Thus $\mathrm{div}(f) = 0$. Conversely, if $\mathrm{div}(f) = 0$, then f has no poles (or zeros) on C. But such a function must be constant, i.e $f \in \bar{K}^\times$. The second part easily follows from the fact that f is a quotient of homogeneous polynomials of the same degree, and thus the number of poles is the same as the number of zeros (counted with multiplicity). □

Definition 2.3.3. Let ϕ be a non-constant rational map between two smooth curves C_1 and C_2. Then ϕ induces a homomorphism $\phi_* : \mathrm{Cl}(C_1) \to \mathrm{Cl}(C_2)$ which we defined as

$$\left[\sum n_i(P_i)\right] \mapsto \left[\sum n_i(\phi(P_i))\right].$$

The map in Definition 2.3.3 will be useful when we consider isogenies of elliptic curves.

Definition 2.3.4. A divisor $D = \sum_{P \in C} n_P(P)$ is called *effective* (or *positive*) if $n_P \geq 0$ for all $P \in C$. In such case we write $D \geq 0$. On the same note, $D_1 \geq D_2$ indicates that $D_1 - D_2$ is effective.
For a divisor D, define

$$\mathcal{L}(D) = \{f \in \bar{K}(C)^\times : \mathrm{div}(f) \geq -D\} \cup \{0\}.$$

Note that $\mathcal{L}(D)$ is a tool for describing zeros or poles of functions. For instance, if $D = 3(P) - (Q)$, then $f \in \mathcal{L}(D)$ means that f can only have a pole of order at most 3 at P and has a zero at P of order at least 1. Note that f has no pole at all points not equal to P.

Proposition 2.3.5. Let $D \in \mathrm{Div}(C)$. Then $\mathcal{L}(D)$ is a vector space over $\bar{K}$.

Proof. Let $f_1, f_2 \in \mathcal{L}(D)$. Then for $c_1, c_2 \neq 0$, we have

$$\begin{aligned}\mathrm{div}(c_1 f_1 + c_2 f_2) &= \sum_{P \in C} \mathrm{ord}_P(c_1 f_1 + c_2 f_2)(P) \\ &\geq \sum_{P \in C} \min\{\mathrm{ord}_P(c_1 f_1), \mathrm{ord}_P(c_2 f_2)\}(P) \\ &\geq -D.\end{aligned}$$

The case cf with $c \in \bar{K}, f \in K(C)^\times$ is not difficult. All the vector space axioms easily follow. □

We denote the dimension of $\mathcal{L}(D)$ by $l(D)$. If C is defined over K and $D \in \mathrm{Div}_K(C)$, then $\mathcal{L}(D)$ has a generating set with functions in $K(C)$, see [8].

Definition 2.3.6. For a curve C, the collection of differential forms Ω_C is the vector space over $\bar{K}$ whose generating set consists of symbols of the form df where $f \in \bar{K}(C)$. The space has the following properties:

a. $d(f+g) = df + dg$ for all $f, g \in \bar{K}(C)$.

b. $d(fg) = f dg + g df$ for all $f, g \in \bar{K}(C)$.

c. $da = 0$ for all $a \in \bar{K}$.

Let $\phi : C_1 \to C_2$ be a non-constant morphism between curves. The corresponding map on function fields $\phi^* : \bar{K}(C_2) \to \bar{K}(C_1)$ induces the following map on differential forms:

$$\phi^* : \Omega_{C_2} \to \Omega_{C_1} \text{ defined by } \left(\sum f_i dy_i\right) \mapsto \sum \phi^*(f) d(\phi^* y_i).$$

Proposition 2.3.7. Let C be a curve.

a. $\dim_{\bar{K}(C)} \Omega_C = 1$.

b. Let $y \in \bar{K}(C)$. Then dy is a basis if and only if $\bar{K}(C)/\bar{K}(y)$ is separable.

c. Suppose $\phi : C_1 \to C_2$ is a non-constant morphism. Then $\phi^* : \Omega_{C_2} \to \Omega_{C_1}$ is one-to-one if and only if ϕ is separable.

Proof. For (a) and (b), see [8].

(c). Choose $y \in \bar{K}(C_2)$ such that dy is a basis for Ω_{C_2}. We know that $\phi^* : \bar{K}(C_2) \to \bar{K}(C_1)$ is injective since ϕ is surjective. By (b), $\bar{K}(C_2)/\bar{K}(y)$ is separable. Now by the identifications $\bar{K}(C_2) \cong \phi^*\bar{K}(C_2)$ and $\bar{K}(y) \cong \phi^*\bar{K}(y)$, it follows that $\phi^*\bar{K}(C_2)/\phi^*\bar{K}(y) = \phi^*\bar{K}(C_2)/\bar{K}(\phi^*y)$ is separable.

Suppose ϕ^* is injective. Then $\phi^*(dy) = d(\phi^*y) \neq 0 \Rightarrow d(\phi^*y)$ is a basis for $\Omega_{C_1} \Rightarrow \bar{K}(C_1)/\bar{K}(\phi^*y) = \bar{K}(C_1)/\phi^*\bar{K}(y)$ is separable $\Rightarrow \bar{K}(C_1)/\phi^*\bar{K}(C_2)$ is separable since $\phi^*\bar{K}(C_2)/\phi^*\bar{K}(y)$ is separable as shown above. Hence ϕ is separable.

Conversely, suppose ϕ is separable. Then $\bar{K}(C_1)/\phi^*\bar{K}(C_2)$ is separable, and so is $\bar{K}(C_1)/\bar{K}(\phi^*y)$ since $\bar{K}(\phi^*y) \subset \phi^*\bar{K}(C_2)$. Then $d(\phi^*y) = \phi^*(dy) \neq 0 \Rightarrow \phi^*$ is injective. □

Let t be a uniformizer at $P \in C$. Then for every $\omega \in \Omega_C$, one can find a unique function $h \in \bar{K}(C)$ such that $\omega = hdt$. This can easily be shown using Propositions 2.1.7 and 2.3.7. We denote h by ω/dt. The value $\mathrm{ord}_P(\omega/dt)$ is called the order of ω at P written $\mathrm{ord}_P(\omega)$. It turns out that $\mathrm{ord}_P(\omega) = 0$ for all but finitely many $P \in C$, see [8].

The preceding proposition will be used quite often to show whether a given map is separable or not in our later discussion on elliptic curves.

Definition 2.3.8. The differential $\omega \in \Omega_C$ is holomorphic if $\mathrm{ord}_P(\omega) \geq 0$ for all $P \in C$. We say it is *non-vanishing* if $\mathrm{ord}_P(\omega) \leq 0$ for all $P \in C$.

We define $\mathrm{div}(\omega) = \sum_{P \in C} \mathrm{ord}_P(\omega)(P)$. Choose any $0 \neq \omega \in \Omega_C$. Since Ω_C is 1-dimensional over $\bar{K}(C)$, $0 \neq \omega_1 \in \Omega_C$ is such that $\omega_1 = f\omega$ for some $f \in \bar{K}(C)$. Hence $\mathrm{div}(\omega) = \mathrm{div}(f) + \mathrm{div}(\omega_1) \Rightarrow \mathrm{div}(\omega) \sim \mathrm{div}(\omega_1)$, i.e we have one divisor class containing all $\mathrm{div}(\omega)$ with $0 \neq \omega \in \Omega_C$. This divisor class in $\mathrm{Cl}(C)$ is called the *canonical divisor class* on C and the divisors $\mathrm{div}(\omega)$ are called canonical divisors.

Denote by $\mathcal{C}$ a canonical divisor on C. Then $\mathcal{C} = \mathrm{div}(\omega)$ for some $0 \neq \omega \in \Omega_C$. Consider $f \in \mathcal{L}(\mathcal{C})$ so that $\mathrm{div}(f) \geq -\mathrm{div}(\omega)$. Then $\mathrm{div}(fw) \geq 0$ which means that $\mathrm{ord}_P(f\omega) \geq 0$ for all $P \in C$, i.e $f\omega$ is holomorphic. Suppose $f\omega$ is holomorphic, then $\mathrm{div}(f\omega) \geq 0 \Rightarrow f \in \mathcal{L}(\mathcal{C})$. Since $\dim_{\bar{K}(C)}\Omega_C = 1$, we have $\mathcal{L}(\mathcal{C}) \cong \{\omega \in \Omega_C : \mathrm{ord}_P(\omega) \geq 0 \text{ for all } P \in C\}$. This shows that $l(\mathcal{C})$ is independent of the choice of $\mathcal{C}$.

Example 2.3.9. We claim that $\Omega_{\mathbb{P}^1}$ has no holomorphic differentials. Let t be a coordinate function. Then $t - \alpha$ is a uniformizer at α and $\mathrm{ord}_\alpha(dt) = \mathrm{ord}_\alpha(d(t-\alpha)) = 0$ and

at $\infty \in \mathbb{P}^1$, we take t^{-1} as our uniformizer. Then

$$\begin{aligned}\operatorname{ord}_\infty(dt) &= \operatorname{ord}_\infty(-t^2 d(t^{-1})) \\ &= \operatorname{ord}_\infty(-(t^{-1})^{-2} d(t^{-1})) \\ &= \operatorname{ord}_\infty(-(t^{-1})^{-2}) + \operatorname{ord}_\infty(d(t^{-1})) = -2.\end{aligned}$$

Hence dt is not holomorphic and that $\operatorname{div}(dt) = -2\infty$.

Let C be a smooth curve. Then $f \in \mathcal{L}(0) \Rightarrow \operatorname{div}(f) \geq 0$. So f has no poles at all $P \in C$ which implies that $f \in \bar{K}$. Thus we must have $\mathcal{L}(0) = \bar{K}$. Now assume that $\deg D < 0$. Then $f \in \mathcal{L}(D)$, i.e $\operatorname{div}(f) \geq -D$ is such that $\deg(\operatorname{div}(f)) > 0 \Rightarrow f = 0 \Rightarrow \mathcal{L}(D) = \{0\}$. Suppose that $D_1 \sim D_2$. Then $D_1 = \operatorname{div}(h) + D_2$ for some $h \in \bar{K}(C)$. Define a map from $\mathcal{L}(D_1)$ to $\mathcal{L}(D_2)$ by $f \mapsto fh$. It can easily be shown that this is an isomorphism of vector spaces, hence $\mathcal{L}(D_1) \cong \mathcal{L}(D_2)$.
In the case when $\deg D = 0$, assume $l(D) \neq \{0\}$. Then there is $f \in \mathcal{L}(D)$ such that $\operatorname{div}(f) + D \geq 0$ and $\deg(\operatorname{div}(f) + D) = 0 \Rightarrow \operatorname{div}(f) + D = 0$. It follows that $D \sim 0 \Rightarrow \mathcal{L}(D) \cong \mathcal{L}(0) = \bar{K} \Rightarrow l(D) = 1$. This shows that $l(D) = 0$ or 1. We have proved the following proposition.

Proposition 2.3.10. Let C be a smooth curve and $D, D_1, D_2 \in \operatorname{Div}(C)$.

a. If $\deg D < 0$, we have $\mathcal{L}(D) = \{0\}$.

b. If $D_1 \sim D_2$, then $\mathcal{L}(D_1) \cong \mathcal{L}(D_2)$.

c. $\mathcal{L}(0) = \bar{K}$ and if $\deg D = 0$, then $l(D) = 0$ or 1.

Theorem 2.3.11. (Riemann-Roch) Let $D \in \operatorname{Div}(C)$ for a smooth curve C. Then there is $g \in \mathbb{Z}_{\geq 0}$ such that

$$l(D) - l(\mathcal{C} - D) = \deg D - g + 1.$$

Proof. Refer to [8]. □

The integer g is called the genus of C. It turns out that for any smooth projective planar curve, $g = \frac{(d-1)(d-2)}{2}$ where d is the degree of the curve [8]. We claim that $g = l(\mathcal{C})$. To see this, set $D = 0$ in Theorem 2.3.11.

According to Example 2.3.9, we note that the genus of $\mathbb{P}^1$ is 0 since there are no holomorphic differentials.

Corollary 2.3.12. We have $\deg(\mathcal{C}) = 2g - 2$ and if $\deg D > 2g - 2$, then $l(D) = \deg D - g + 1$.

Proof. Using Theorem 2.3.11, let $D = \mathcal{C}$. Then $l(\mathcal{C}) - l(0) = \deg \mathcal{C} - g + 1$, and $g = l(\mathcal{C}) \Rightarrow \deg(\mathcal{C}) = 2g - 2$. For the second part, we have $\deg(\mathcal{C} - D) = \deg \mathcal{C} - \deg D < 0$. By Proposition 2.3.10 (a), it follows that $l(\mathcal{C} - D) = 0$. So $l(\mathcal{C} - D) - l(\mathcal{C} - (\mathcal{C} - D)) = \deg(\mathcal{C} - D) - g + 1 = \deg \mathcal{C} - \deg D - g + 1$ by Theorem 2.3.11, and the result follows. □

As a consequence, note that for a genus one curve with $\deg D > 0$, Corollary 2.3.12 says that $l(D) = \deg(D)$.

Proposition 2.3.13. Let C be a smooth curve with $g \geq 1$. Let $P, Q \in C$. Then $(P) \sim (Q) \Rightarrow P = Q$.

Proof. By assumption, there is $f \in \bar{K}(C)$ such that $\operatorname{div}(f) = (P) - (Q)$. Suppose that $P \neq Q$. Now for $r \geq 0$, $\operatorname{div}(f^r) = r(P) - r(Q)$. The function f^r has a pole of order r at Q and so $f^r \in \mathcal{L}(rQ)$. Since $\deg((2g-1)(Q)) = 2g - 1 > 2g - 2$, we have $\dim_{\bar{K}} \mathcal{L}((2g-1)(Q)) = g$ by Corollary 2.3.12. The set $\{1, f, f^2, \ldots, f^{2g-1}\}$ is linearly independent in $\mathcal{L}((2g-1)(Q))$ since functions have different pole order at Q. Hence the subspace they span has dimension $2g$ which is greater than $\dim_{\bar{K}} \mathcal{L}((2g-1)(Q))$. This is a contradiction. So we must have $P = Q$. □

Chapter 3

Basics of Elliptic Curves

The references [8] and [10] are used in this chapter.
We discuss some geometry of elliptic curves and their morphisms.

Definition 3.0.14. An affine cubic curve $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ with $a_i \in \bar{K}$ is said to be in (generalized) *Weierstrass* form. The same definition applies to projective cubic curves. Sometimes we use $E(x, y)$ to denote the defining polynomial of E.

Observe that $E(x, y)$ is irreducible, i.e $I(E)$ is a prime ideal in $\bar{K}[x, y]$. To see this, assume that the polynomial is reducible over $\bar{K}(x)[y]$, i.e $E(x, y) = (y + f)(y + g)$ where $f, g \in \bar{K}(x)$. Comparing the coefficients, we have

$$fg = -x^3 - a_2x^2 - a_4x - a_6 \quad \text{and} \quad f + g = a_1x + a_3.$$

Taking the degrees (the usual degree function on rational functions), we note that $\deg(f + g) \leq 1$ and $\deg(fg) = \deg f + \deg g = 3$. But we also have

$$1 \geq \deg(f + g) = \max\{\deg f, \deg g\} \geq \frac{1}{2}(\deg f + \deg g) = \frac{3}{2}$$

which is a contradiction. Hence $E(x, y)$ is irreducible over $\bar{K}(x)[y]$ and therefore irreducible over $\bar{K}[x, y]$.
We relate the following quantities to E or $\overline{E}$:

The quantities j, Δ, and ω are called the *j-invariant*, the *discriminant* and the *invariant*

$b_2 = a_1^2 + 4a_2 \quad b_4 = 2a_4 + a_1a_3 \quad b_6 = a_3^2 + 4a_6$
$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 \quad c_4 = b_2^2 - 24b_4$
$c_6 = -b_2^3 + 36b_2b_4 - 216b_6 \quad \Delta = -b_2^2b_8 - 8b_4 - 27b_6^2 + 9b_2b_4b_6$
$j = \frac{c_4^3}{\Delta}$ for $\Delta \neq 0$
$\omega = \frac{dx}{2y+a_1x+a_3} = \frac{dy}{3x^2+2a_2x+a_4-a_1y}$

differential, respectively.

We observe that

$$\Delta = \frac{c_4^3 - c_6^2}{1728} \text{ and } 4b_8 = b_2b_6 - b_4^2 \tag{3.0.1}$$

Definition 3.0.15. Two cubic curves $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ and $E' : y'^2 + a_1'x'y' + a_3'y' = x'^3 + a_2'x'^2 + a_4'x' + a_6'$ are said to be isomorphic (up to preserving the Weierstrass equation and fixing the origin) if there exists a transformation $E \to E'$ defined by $x = u^2x' + r, y = u^2sx' + u^3y' + t$ with $u \in \bar{K}^\times, r, s, t \in \bar{K}$. Such a transformation is called an *admissible change of variables*.

Under admissible change of variables with the notation in Definition 3.0.15, the relationship between coefficients a_i and a_i' is highlighted in Table 3.1.

$a_1' = u^{-1}(a_1 + 2s)$
$a_2' = u^{-2}(a_2 - sa_1 + 3r - s^2)$
$a_3' = u^{-3}(a_3 + ra_1 + 2t)$
$a_4' = u^{-4}(a_4 + 2ra_2 - (rs + t)a_1 - sa_3 + 3r^2 - 2st)$
$a_6' = u^{-6}(a_6 + r^2a_2 + ra_4 - rta_1 - ta_3 + r^3 - t^2)$
$b_2' = u^{-2}(b_2 + 12r)$
$b_4' = u^{-4}(b_4 + rb_2 + 6r^2)$
$b_6' = u^{-6}(b_6 + 2rb_4 + r^2b_2 + 4r^3)$
$b_8' = u^{-8}(b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4)$
$c_4' = u^{-4}c_4, \quad \Delta' = u^{-12}\Delta$
$j' = j$

Table 3.1: Admissible change of variables

If char $\bar{K} \neq 2$, then under the transformation $y \mapsto \frac{1}{2}(y - a_1x - a_3)$, $E(x, y) = 0$ becomes $y^2 = 4x^3 + b_2x^2 + b_4x + b_6$ for some constants $b_2, b_4, b_6 \in \bar{K}$. Applying $(x, y) \mapsto (x, 2y)$ gives an equation of the form $y^2 = x^3 + e_2'x^2 + e_4'x + e_6'$ for some constants e_2, e_4 and e_6. If we further assume that char $\bar{K} \neq 3$, then applying $(x, y) \mapsto \left(x - \frac{1}{3}e_2', y\right)$ results in the equation $y^2 = x^3 + Ax + B$ for some $A, B \in \bar{K}$.

If char $K = 2$ with $a_1 = 0$, then applying $x \mapsto x + a_2$ to $E(x, y) = 0$ yields $y^2 + a_3''y =$

$x^3+a_4''x+a_6''$. On the other hand, when $a_1 \neq 0$, we obtain the form $y^2+xy = x^3+a_2'''x^2+a_6'''$ under the map $(x,y) \mapsto \left(a_1^2x + \frac{a_3}{a_1}, a_1^3y + \frac{a_1^2a_4+a_3^2}{a_1^3}\right)$.

Proposition 3.0.16. Let E be a projective cubic curve in Weierstrass form as before. Then E is non-singular if and only if $\Delta \neq 0$.

Proof. E is given by the equation $Y^2Z+a_1XYZ+a_3YZ^2 = X^3+a_2X^2Z+a_4XZ^2+a_6Z^3$, and has only one point at infinity; [0:1:0]. We note that this point is non-singular. For the rest of the points, we use the standard affine patch by dehomogenising $\overline{E}(X,Y,Z)$ with respect to Z. We explore two cases in which the characteristic of the field K is distinguished.

For $\operatorname{char} K \neq 2$, it is enough to consider the equation of the form $y^2 = f(x)$ where $f(x) = x^3 + a_2x^2 + a_4x + a_6$. Now $(x,y) \in E$ is singular if and only if $y = 0$ and $f'(x) = 0$, i.e $f(x) = 0$ and $f'(x) = 0 \Rightarrow \Delta = 0$.

If $\operatorname{char} K = 2$, we consider the following situations:

Suppose we have the form $E : y^2 + xy = x^3 + a_2x^2 + a_6$, $\Delta = a_6$. We note that (x,y) is singular if and only if $x = y = 0$, and $E(x,y) = 0 \Rightarrow a_6 = 0$.

On the other hand, for the form $E : y^2 + a_3y = x^3 + a_4x + a_6$, $\Delta = a_3^2$, the only singular point is $(\sqrt{a_4}, \sqrt{a_6})$ and occurs when $a_3 = 0$. In either case, the result holds. □

It can be shown that if E is a singular cubic curve in Weierstrass form, then E is birationally isomorphic to the $\mathbb{P}^1$.

Definition 3.0.17. An *elliptic curve* over K is a smooth genus one curve with at least one point having coordinates in K.

Proposition 3.0.18. Let E be an elliptic curve over K. Then E is isomorphic to a curve in Weierstrass form with coefficients in K.

Proof. Let O be a base point of E. Then $l(n(O)) = n$ for $n \geq 1$. Now $l((O)) = 1$. Since $l(2(O)) > l((O))$, there is $x \in K(C)^\times$ such that x has a double pole at O and no poles elsewhere. Similarly since $l(3(O)) > l(2(O))$, there is $y \in K(C)^\times$ with a triple pole at O and no poles elsewhere. Note that $\mathcal{L}(6(O))$ has 6 basis elements but contains $\{1, x, y, y^2, x^3, x^2, xy\}$. So there are $b_1, b_2, b_3, b_4, b_5, b_6, b_7 \in K$, not all zero, such that $b_1y^2 + b_2xy + b_3y = b_4x^3 + b_5x^2 + b_6x + b_7$. If $b_1 = 0$, then $b_i = 0$ for all $i \neq 1$ since

$\{1, x, y, x^3, x^2, xy\}$ is linearly independent. Hence $b_1 \neq 0$. Similarly $b_4 \neq 0$. Scaling down the coefficients we obtain an equation of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Denote by E' the projective closure of the above cubic curve. Let $\psi : E \to \mathbb{P}^1$ be defined by $\psi = [x, y, 1]$. As $x, y \in K(E)$, $\psi : E \to E'$ is a morphism. Note that $\psi(O) = [0 : 1 : 0]$. This is because $x = t^{-2}u$ and $y = t^{-3}v$ where $u, v \in \mathcal{O}_O(E)^\times$ and t is a uniformizer at O. By Proposition 2.2.4, ψ is surjective. It turns out that $[K(E) : K(x, y)] = 1$, see [8]. Hence ψ is a degree 1 map.

To finish the proof, we just need to show that E' is smooth. Assume E' is singular. Then there is a birational isomorphism $\eta : E' \to \mathbb{P}^1$ of degree 1. Now the composition $\eta \circ \psi : E \to \mathbb{P}^1$ is a degree 1 map implying that E has genus 0. This is a contradiction and so E' is smooth. Thus $E \cong E'$. □

It also turns out that every projective smooth cubic curve over K and in Weierstrass form defines an elliptic curve over K. It is easy to see that such an equation will always have at least one point with coordinates in K. Furthermore its genus is 1 since it is smooth and has degree 3. This settles the matter because $g = \frac{(d-1)(d-2)}{2} = 1$.

By some transformation, an elliptic curve defined over K where $\operatorname{char} K \neq 2, 3$, we have the form $y^2 = x^3 + Ax + B$. Using equations in 3.0.1, the j-invariant can be written as

$$j = 1728\frac{4A^3}{4A^3 - 27B^2}.$$

This form is convenient computationally and will be used in most cases.

Proposition 3.0.19. Let $\operatorname{char} K \neq 2, 3$.

(a) Two elliptic curves are isomorphic if and only if they have the same j-invariant.

(b) There exists for any $j \in \bar{K}$, an elliptic curve defined over $K(j)$ that is isomorphic to an elliptic curve with j as its j-invariant.

Proof. If two elliptic curves are isomorphic, then clearly they have the same j-invariant as formulas in Table 3.1 can tell.

Conversely, suppose that char $K \neq 2, 3$ and $j(E) = j(E')$. We can write $E : y^2 = x^3 + \gamma_1 x + \beta_1$ and $E' : y'^2 = x'^3 + \gamma_2 x + \beta_2$. Now $j(E) = 1728\frac{4\gamma_1^3}{4\gamma_1^3+27\beta_1^2} = j(E') = 1728\frac{4\gamma_2^3}{4\gamma_2^3+27\beta_2^2} \Leftrightarrow \gamma_1^3\beta_2^2 = \gamma_2^3\beta_1^2$. It is not difficult to see that an admissible change of variables between the two curves is only one of the form $(x, y) \mapsto (u^2x', u^3y')$. We look at the following cases:

Case I: $\beta_1 = 0$ in which case $\gamma_1 \neq 0$ ($j(E) = 1728$) since $\Delta(E) \neq 0$. So we must have $\beta_2 = 0$ and $\gamma_2 \neq 0$. Setting $u = (\gamma_1/\gamma_2)^{1/4}$ gives the isomorphism.

Case II: $\gamma_1 = 0$ ($j(E) = 0$) which implies $\beta_1 \neq 0$ since $\Delta(E) \neq 0$. Then we must have $\gamma_2 = 0$, otherwise we will not have $j(E') = 0$ and furthermore, $\beta_2 \neq 0$. We note that $u = (\beta_1/\beta_2)^{1/6}$ gives the isomorphism.

Case III: $\gamma_1\beta_1 \neq 0$ so that $j \neq 1728, 0$. Then both γ_2 and β_2 are not equal to zero. So $u = (\gamma_1/\gamma_2)^{1/4}$ or $(\beta_1/\beta_2)^{1/6}$ gives the required isomorphism. For (b), see [8]. □

3.1 The Group Law

Let E be an elliptic curve defined over K. Choose a K-rational point O. We define a binary operation $+$ on E as follows:

For $P, Q \in E$, let l be the straight line passing through P and Q. Let R be the third point of intersection of l with E. Let l' be the straight line intersecting E at O and R. Then we set $P + Q$ to be the third point of intersection of l' with E. Note that any line must intersect with E at exactly three points (counting multiplicities) as a consequence of Bezout's theorem.

Proposition 3.1.1. The binary operation $+$ above satisfies the following properties:

a. For any $P, Q, R \in l \cap E$, we have $P + Q + R = O$.

b. $P + Q = Q + P$.

c. $P + O = P$ for all $P \in E$.

d. For all $P \in E$, there exist $P' \in E$ such that $P + P' = O$.

e. $(P + Q) + R = P + (Q + R)$ for all $P, Q, R \in E$.

Proof. Statements (a) and (b) are obvious. We note that the lines l and l' coincide when we set $Q = O$ in the definition for $P + Q$. Consequently (c) follows.
For (d), replace Q by O in (a) so that $P + O + R = O$. By (b), we have $P + R = O$, so set $P' := R$.
We postpone the proof of associativity. We will prove it by showing that $\mathrm{Cl}^0(E) \cong (E, +)$. To achieve this, we need the following ideas. □

Proposition 3.1.2. Let E be an elliptic curve and $O \in E$. Let $D \in \mathrm{Div}^0(E)$. Then there is a unique point $P \in E$ such that $D \sim (P) - (O)$. This induces a surjective map $\rho : \mathrm{Div}^0(E) \to E$ defined by $D \mapsto P$.

Proof. Clearly $\deg(D + (O)) = 1 \Rightarrow l(D + (O)) = 1$ by Corollary 2.3.12. So there is $f \in \bar{K}(E)$ such that $\mathrm{div}(f) \geq -D-(O)$. But $\deg(\mathrm{div}(f)) = 0 \Rightarrow \mathrm{div}(f) = -D-(O)+(P)$ for some $P \in E \Rightarrow D \sim (P) - (O)$. If $Q \in E$ with $D \sim (Q) - (O)$, then we have $(Q) \sim (P)$. The curve E has genus 1 and by Proposition 2.3.13, $P = Q$. The map ρ is surjective because for every $P \in E$, we can construct a 0-degree divisor $(P) - (O)$ satisfying $\rho((P) - (O)) = P$. □

It is also not difficult to see that under ρ, two divisors are mapped to the same point on E if and only if they are linearly equivalent. Hence ρ induces an isomorphism $\mathrm{Cl}^0 \to E$ given by $[(P)-(O)] \mapsto P$. Let κ denote the inverse of this map so that $\kappa : E \to \mathrm{Cl}^0$, $P \mapsto [(P) - (O)]$.

Proposition 3.1.3. For an elliptic curve E, let $D = \sum_{P \in E} n_P(P) \in \mathrm{Div}(E)$. Then D is principal if and only if $\sum_{P \in E} n_P P = O$ and $\sum_{P \in E} n_P = 0$.

Proof. See [8]. □

Proposition 3.1.4. Let an elliptic curve E be given by a Weierstrass equation. The map κ as given above is a group homomorphism.

Proof. Let $O = [0 : 1 : 0]$, and say $P, Q \in E$. It suffices to show that $(P)+(Q)-(P+Q)-(O) \in \mathrm{Prin}(E)$. Let $l, l' \subset \mathbb{P}^2$ be lines such that $l \cap E = \{P, Q, R\}$ and $\{R, O\} \in l' \cap E$. Denote by $f = b_0X + b_1Y + b_2Z$ and $f' : b'_0X + b'_1Y + b'_2Z$ the defining polynomials of l

and l', respectively. By construction and definition of group law, we have

$$\text{div}\left(\frac{f'}{Z}\right) = (P+Q)+(R)-2(O) \text{ and } \text{div}\left(\frac{f}{Z}\right) = (P)+(Q)+(R)-3(O)$$

which yields $\text{div}\left(\frac{f'}{f}\right) = (P)+(Q)-(P+Q)-(O) \in \text{Prin}(E)$. □

Therefore associativity of the elliptic curve group law follows from the homomorphism. We claim that the set of K-rational points on E/K given by

$$E(K) = \{(x,y) \in K^2 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{[0:1:0]\}$$

is a subgroup of E. To see this, let $O = [0:1:0]$. If $P, Q \in E(K)$ are affine points, then the third point of intersection of l with E will have coordinates in K and that a projective line through the third point and $[0:1:0]$ has to intersect E at third point with coordinates in K. Consequently $P+Q \in E(K)$.

Now we derive the explicit addition formulas for the group law. We look at the case when char $K \neq 2, 3$. Other cases can be similarly explored. The addition with the origin $O = [0:1:0]$ is geometrically illustrated in the Figure 3.1.

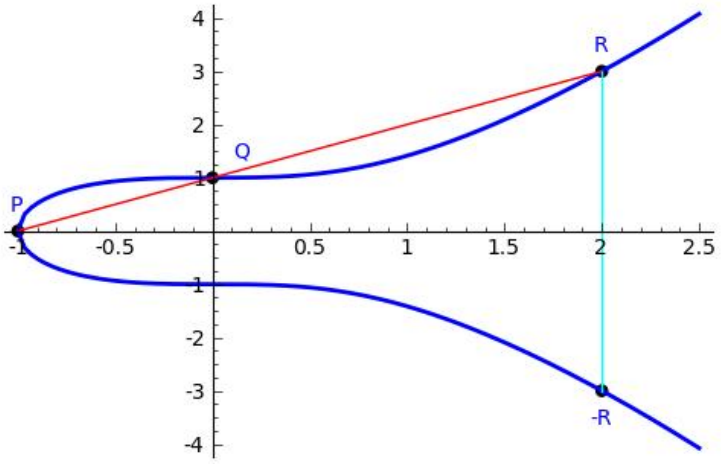


Figure 3.1: Elliptic Curve Point Addition

On an elliptic curve given by $y^2 = x^3 + Ax + B$, we see that if $P = (x_1, y_1)$ then $-P = (x_1, -y_1)$. If you want to add P and Q where $x(P) \neq x(Q)$, then find the line passing through P and Q. From Bezout's theorem, it meets in three points: P, Q and R. So $P+Q+R = O$. Thus $P+Q = -R$. To double a point, find the tangent line. From

Bezout's theorem, it meets in three points P, P and R. Thus $2P = -R$.

The geometric intuition of addition can now be transformed into algebra. Let $P = (x_1, y_1)$, $Q = (x_2, y_2)$ and $P + Q = S = (x_3, y_3)$. Let $P = (x_1, y_1)$, $Q = (x_2, y_2)$ and $P + Q = S = (x_3, y_3)$, we derive some rules for obtaining x_3 and y_3 from A, B and the coordinates of P and Q.

Suppose $x_1 \neq x_2$. Let $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$. The equation of the straight line passing through P and Q is obtained from the equation $\dfrac{y - y_1}{x - x_1} = \lambda$ or $y = \lambda(x - x_1) + y_1$. We replace the y in $y^2 = x^3 + Ax + B$ by $\lambda(x - x_1) + y_1$ and get $0 = x^3 - (\lambda^2)x^2 + \ldots$. The roots of this cubic give the x-coordinates of P, Q and $-S = (x_3, -y_3)$. So $x_1 + x_2 + x_3 = \lambda^2$ and $x_3 = \lambda^2 - x_1 - x_2$. Thus $y_3 = \lambda(x_1 - x_3) - y_1$. On the other hand, if $x_1 = x_2$ we have two cases: the case where $y_1 = -y_2$ and the case where $y_1 \neq -y_2$, in which case $y_1 = y_2$. We have seen that the first case means $P = -Q$ and so $P + Q = O$. In the second case, $P = Q$. The tangent line to the elliptic curve at Q has intersection multiplicity at least 2 at P, so we use it. The equation of the tangent line is $y = \frac{dy}{dx}(x_1, y_1)(x - x_1) + y_1$. Using implicit differentiation, $\frac{dy}{dx}(x_1, y_1) = \frac{3x_1^2 + A}{2y_1}$. So $x_3 = \lambda^2 - x_1 - x_2$ and $y_3 = \lambda(x_1 - x_3) - y_1$ with $\lambda = \frac{3x_1^2 + A}{2y_1}$.

Incorporating the computations we have just made, the group law for an elliptic curve in the form $y^2 = x^3 + Ax + B$ is defined below.

In the rule below, if P is not O we let $P = (x_1, y_1)$, if Q is not O we let $Q = (x_2, y_2)$ and if $S = P + Q$ is not O we let $S = (x_3, y_3)$.

i. $P + O = P + O = P$.

ii. We define $-O = O$. If $P \neq O$, we define $-P = (x_1, -y_1)$. So if $P = Q$ and $y_1 = 0$, then $P + Q = O$. Also for $x_1 = x_2$ and $y_1 \neq y_2$, $P + Q = O$.

iii. If $x_1 \neq x_2$ then $x_3 = \lambda^2 - x_1 - x_2$ and $y_3 = \lambda(x_1 - x_3) - y_1$ where $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$.

iv. If $P = Q$ and $y_1 \neq 0$ we have $x_3 = \lambda^2 - x_1 - x_2$, $y_3 = \lambda(x_1 - x_3) - y_1$ where $\lambda = \frac{3x_1^2 + A}{2y_1}$.

Example 3.1.5. Let $E/\mathbb{C}$ be given by the equation $y^3 = x^3 + 2x + 1$. We would like to add the points $P = (-7/16, 13/64)$ and $Q = (0, 1)$.

We have $\lambda = 51/28$ and $x_1 = 0, x_2 = -7/16, y_1 = 1, y_2 = 13/64$. Then $x_3 = \lambda^2 - x_1 - x_2 = 184/49$ and $y_3 = \lambda(x_1 - x_3) - y_1 = -2689/343$. So $P + Q = (184/49, -2689/343)$.

Example 3.1.6. Let α be a root of the polynomial $x^2 + x + 1 \in \mathbb{F}_2[x]$ and $E/\mathbb{F}_{2^2}$ defined by $y^2 + xy = x^3 + x^2 + (\alpha + 1)x + 1$. We want to find $2(\alpha + 1, 0)$. We compute

$$\lambda = \frac{dy}{dx} = \frac{3x^2 + 2x + \alpha + 1 - y}{2y + x} = \frac{x^2 + \alpha + 1 + y}{x}$$

and at $x = \alpha + 1$, we have $\lambda = \frac{(\alpha+1)^2+\alpha+1}{\alpha+1} = \frac{1}{\alpha+1} = \alpha$. The tangent line at $(\alpha + 1, 0)$ is $y = \alpha x + 1$. To find the value of the x-coordinate of the third point, we solve the equation

$$(\alpha x + 1)^2 + x(\alpha x + 1) = x^3 + x^2 + (\alpha + 1)x + 1$$

which yields $x = 0$ and $\alpha + 1$(twice). Hence $2(\alpha + 1, 0) = (0, 1)$.

It was earlier claimed that for a smooth curve C, the local ring $\mathcal{O}_P(C)$ is a discrete valuation ring, we now prove the claim for elliptic curves by explicitly computing the uniformizers. From the affine equation of an elliptic curve $E : Y^2 + a_3XY + a_1Y = x^3 + a_2x^2 + a_4X + a_6$, it is clear that $K(E) = \frac{K(X)[Y]}{\langle E(X,Y)\rangle}$ is a quadratic extension of $K(X)$. We also note that $f \in K(E)$ can be written as $f = w_1 + w_2Y$ for some $w_1, w_2 \in K(X)$. We define $\overline{X} = X$ and $\overline{Y} = -Y - a_1X - a_3$. We define the norm $N : K(E) \to K(X)$ by $f \mapsto f\bar{f}$.

Let $h \in \mathcal{O}_P(E)$. Then $h = \frac{h_1}{h_2}$ where $h_2(P) \neq 0$. Thus h_2 is a unit in $\mathcal{O}_P(E)$. If $h_1(P) \neq 0$, then h_1 is also a unit and if t is a uniformizer at P, then $\operatorname{ord}_P h = 0$. Now we assume that $h_1(P) = 0$ and let s represent the order of a function at P.

Suppose $P = (x, y)$ is not a point of order 2. Then $u = X - x$ is a uniformizer. We have $h_1 = w_1 + w_2Y$ with $w_1, w_2 \in K[X]$. We can thus write $h_1 = (X - x)^{s_0}(w_1' + w_2'Y)$ where w_1' and $w_2'Y$ have no common factor in $X - x$, i.e $w_1'(x) \neq 0$ or $w_2'(x) \neq 0$. Set $h_1' = w_1' + w_2'Y$.

If $h_1'(P) \neq 0$, then h_1 is a unit in the local ring, and so $s = s_0$.

If $\overline{h_1'}(P) \neq 0$, then $\overline{h_1'}$ is a unit and so $h_1' = N(h_1)(\overline{h_1'})^{-1} = (X - x)^{s_1}h_1''(\overline{h_1'})^{-1}$ with $h_1'' \in K[X]$ and $h_1''(x) \neq 0$. So $s = s_0 + s_1$.

Suppose that $h_1'(P) = \overline{h_1'}(P) = 0$. Then $(v, t) = (w_1'(x), w_2'(x))$ is a solution to following

system of equations

$$\begin{pmatrix} 1 & Y(P) \\ 1 & \overline{Y}(P) \end{pmatrix} \begin{pmatrix} v \\ t \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

Since P is not a point of order 2, we have $\overline{Y}(P) \neq Y(P)$ so that the system above has only the trivial solution. But this is a contradiction as we cannot have both $w_1'(x) = 0$ and $w_2'(x) = 0$.

Suppose P is a point of order 2 and char $K \neq 2$. We can apply an admissible change of variables and put the curve in the form $E : Y^2 = X^3 + a_2X^2 + a_4X + a_6$ and $P = (r_1, 0)$. We claim that Y is a uniformizer at P.

Clearly $X - r_1 = \frac{(X-r_1)(X-r_2)(X-r_3)}{(X-r_2)(X-r_3)}$ where r_2 and r_3 are the two other roots of the polynomial $X^3 + a_2X^2 + a_4X + a_6$. So we have $X - r_1 = \frac{Y^2}{(X-r_2)(X-r_3)}$. Note that $(X - r_2)(X - r_3)$ is a unit in $\mathcal{O}_P(E)$. Now

$$h_1(P) = 0 \Rightarrow h_1 = (X - r_1)^{s_2} f = \frac{Y^{2s_2}}{(X - r_2)^{s_2}(X - r_3)^{s_2}} f$$

for some $f \in K[E]$. Now $f = w + uY$ where $w, u \in K[X]$ and $w(r_1) \neq 0$ or $u(r_1) \neq 0$. If $f(P) \neq 0$, then $s = 2s_2$. Otherwise, we must have $w(r_1) = 0$ and $u(r_1) \neq 0$. Thus $w(x) = (X - r_1)u_1$ with $u_1 \in K[X]$ so that

$$\begin{aligned} f = (X - r_1)u_1 + uY &= \frac{(X - r_1)(X - r_2)(X - r_3)u_1 + u(X - r_2)(X - r_3)Y}{(X - r_2)(X - r_3)} \\ &= Y\frac{u_1Y + u(X - r_2)(X - r_3)}{(X - r_2)(X - r_3)}. \end{aligned}$$

Hence $s = 2s_2 + 1$

Finally suppose that $P = (x, y)$ has order 2 and char $K = 2$. We know that $y = \overline{Y}(P) = -y - a_1x - a_3$. There are two possible situations:

Consider $E : Y^2 + XY = X^3 + a_2X^2 + a_6$. Then $\Delta = a_6 \neq 0$ ($j \neq 0$) and $a_1 = 1$. From the equation $y = -y - a_1x - a_3$, we obtain $2y = x = 0 \Rightarrow P = (0, y)$ with $y^2 = a_6$. A uniformizing parameter is given by $Y + y$. As it was in the previous case, we have

$$X = (Y + y)^2\frac{X}{(Y + y)^2} = (Y + y)^2\frac{X}{(Y^2 + a_6)}$$

which is equal to

$$(Y + y)^2\frac{X}{X^3 + a_2X^2 + XY} = (Y + y)^2\frac{1}{X^2 + a_2X + Y}.$$

Note that $X^2 + a_2X + Y$ is a unit in the local ring. Thus we can write $h_1 = X^{s_3}f$ where $f = w + u(Y + y)$ for some $w, u \in K[X]$ and not both $w(0)$ and $u(0)$ are zero. So $h_1 = (Y + y)^{2s_3}\frac{1}{(X^2+a_2X+Y)^{s_3}}f$. If $f(P) \neq 0$, we are done and $s = 2s_3$. Otherwise, $w(0) = 0$, so $w(x) = Xw_2$ and $u(0) \neq 0$. Hence

$$\begin{aligned} f = Xw_2 + u(Y + y) &= \frac{(Y + y)^2w_2}{X^2 + a_2X + Y} + u(Y + y) \\ &= (Y + y)\frac{(Y + y)w_2 + u(X^2 + a_2X + Y)}{X^2 + a_2X + Y} \end{aligned}$$

in which case $s = 2s_3 + 1$.

The above computations are relevant when P is finite. When P is not finite, i.e $P = O$, we would like to find a uniformizer there. Recall the equation in projective coordinates

$$E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4X^2Z + a_6Z^3.$$

We claim that a uniformizer at O is given by $u = \frac{X}{Y}$. Dehomogenizing E with respect to Y gives $E' : Z + a_1XZ + a_3Z^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$. Since homogenisation and dehomogenization are inverse field isomorphisms, we need to show that $u' = X$ is a uniformizer at $(0, 0)$. Notice that

$$\begin{aligned} Z = \frac{ZX^3}{X^3} &= \frac{ZX^3}{Z + a_1XZ + a_3Z^2 - a_2X^2Z - a_4XZ^2 - a_6Z^3} \\ &= X^3\frac{1}{1 + a_1X + a_3Z - a_2X^2 - a_4XZ - a_6Z^2}. \end{aligned}$$

Note that $\frac{1}{1+a_1X+a_3Z-a_2X^2-a_4XZ-a_6Z^2}$ is a unit in the local ring at $(0, 0)$. For any polynomial $f \in K[E]$, we have $f = p(Z) + q(Z)X + w(Z)X^2$ where $p, q, w \in K[Z]$. We can further write $f = p_1(Z)Z^i + q_1(Z)XZ^j + w_1(Z)X^2Z^k$ where each one of p_1, q_1 and w_1 is either zero or not divisible by Z. When Z is replaced by $\frac{X^3}{1+a_1X+a_3Z-a_2X^2-a_4XZ-a_6Z^2}$, we find that

$$f = p_2(X, Z)X^{3i} + q_2(X, Z)X^{3j+1} + w_2(X, Z)X^{3k+2}$$

where p_2, q_2 and w_2 are regular rational functions and are; either the zero polynomial or not zero at $(0, 0)$. Let $\tilde{s} = \min\{3i, 3j + 1, 3k + 2\}$. Then $f = X^{\tilde{s}}f_1$ where f_1 is regular and not zero at $(0, 0)$, and so $s = \tilde{s}$. We conclude that $\frac{X}{Y}$ is a uniformizer at O.

3.2 Isogenies and the torsion structure

Unless otherwise stated, E denotes an elliptic curve and O its zero point.

Definition 3.2.1. Let E_1 and E_2 be elliptic curves with O_1 and O_2 as zero points, respectively. A morphism $\psi : E_1 \to E_2$ is called an *isogeny* if $\psi(O_1) = O_2$. The set of isogenies from E onto itself is denoted $\mathrm{End}(E)$. Addition and multiplication in $\mathrm{End}(E)$ are given by

$$(\psi + \phi)(P) = \psi(P) + \phi(P) \text{ and } (\psi\phi)(P) = \psi(\phi(P)), \text{ respectively.}$$

One sees that $\mathrm{End}(E)$ is a ring. We call this ring the endomorphism ring of E. Given E/K, we denote $\mathrm{End}_K(E)$ those endomorphisms defined over K. Let $m \in \mathbb{Z}$.
The multiplication by m map $[m]$ is defined by

$$[m]P = \begin{cases} \underbrace{P + P + \ldots + P}_{m \text{ times}} & \text{if } m > 0 \\ \underbrace{-P - P - \ldots - P}_{-m \text{ times}} & \text{if } m < 0. \end{cases}$$

The map $[m]$ is an endomorphism since it can be given by rational functions obtainable via group law formulas and $[m](O) = m(O) = O$. Note that $[m]$ is not zero for $m \neq 0$. We also define $\deg[0] = 0$.
We say that an elliptic curve E has complex multiplication (CM) if $\mathrm{End}(E)$ is strictly greater than $\mathbb{Z}$. For instance, all elliptic curves defined over finite fields are CM curves and the Frobenius morphism provides an extra endomorphism.

Proposition 3.2.2. An isogeny $\psi : E \to E'$ is a group homomorphism, i.e. $\psi(P+Q) = \psi(P) + \psi(Q)$.

Proof. Let $\kappa_1 : E \to \mathrm{Cl}^0(E)$ and $\kappa_2 : E' \to \mathrm{Cl}^0(E')$ be the maps $P \mapsto [(P) - (O)]$ and $P \mapsto [(P) - (O')]$. As already shown, these maps are isomorphisms of groups. We also know that the map $\psi_* : \mathrm{Cl}^0(E) \to \mathrm{Cl}^0(E')$ is a homomorphism (from Definition 2.3.3 where we restrict to degree zero divisor classes). Since $(\psi_* \circ \kappa_1)(P) = \psi_*([(P) - (O)]) = [(\psi(P)) - (O')] = \kappa_2(\psi(P)) = (\kappa_2 \circ \psi)(P)$, the following diagram commutes

$$\begin{array}{ccc} E & \xrightarrow[\kappa_1]{\cong} & \mathrm{Cl}^0(E) \\ \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \psi_*} \\ E' & \xrightarrow[\kappa_2]{\cong} & \mathrm{Cl}^0(E') \end{array}$$

So $\psi = \kappa_2^{-1} \circ \psi_* \circ \kappa_1 \Rightarrow \psi$ is a group homomorphism. □

On an elliptic curve, we will denote the translation-by-Q map by τ_Q, i.e $\tau_Q(P) = P + Q$. Note that this is a rational map.

Lemma 3.2.3. Let Q be a point on E. Then τ_Q is unramified.

Proof. Let id denote the identity map. Obviously τ_{-Q} is the inverse of τ_Q. Let $P \in E$. So $e_{\tau_Q \circ \tau_{-Q}}(P) = e_{\mathrm{id}}(P) = 1$. But by Proposition 2.2.7, $e_{\tau_{-Q} \circ \tau_Q}(P) = e_{\tau_Q}(P) e_{\tau_{-Q}}(\tau_Q(P)) = e_{\tau_Q}(P) e_{\tau_{-Q}}(P + Q)$ so that $e_{\tau_Q}(P) e_{\tau_{-Q}}(P + Q) = 1 \Rightarrow e_{\tau_Q}(P) = 1$. □

Proposition 3.2.4. Let $\phi \in \mathrm{End}(E)$. Then $e_\phi(P)$ is the same for all $P \in E$.

Proof. Fix a point $P \in E$. Let $Q \in E$. Then $\phi(\tau_P(Q)) = \phi(Q + P) = \phi(Q) + \phi(P) = \tau_{\phi(P)}(\phi(Q))$. So we have $\phi \circ \tau_P = \tau_{\phi(P)} \circ \phi$.
By Proposition 2.2.7, we know that $e_{\phi \circ \tau_P}(O) = e_{\tau_P}(O) e_\phi(\tau_P(O)) = e_{\tau_P}(O) e_\phi(P)$ which implies $e_\phi(P) = \frac{e_{\phi \circ \tau_P}(O)}{e_{\tau_P}(O)}$. By Lemma 3.2.3, $e_{\tau_P}(O) = 1$ so that $e_\phi(P) = e_{\phi \circ \tau_P}(O) \Rightarrow e_\phi(P) = e_{\tau_{\phi(P)} \circ \phi}(O) = e_\phi(O) e_{\tau_{\phi(P)}}(O) = e_\phi(O)$. Since P was chosen arbitrarily, the result holds. □

Set $e_\phi := e_\phi(P)$ where P is any point on E. Then we note that for any $\phi, \psi \in \mathrm{End}(E)$, we have

$$e_{\phi \circ \psi}(P) = e_\psi(P) e_\phi(\psi(P)) = e_\psi(P) e_\phi(P),$$

i.e $e_{\phi \circ \psi} = e_\phi e_\psi$.

Example 3.2.5. Let $K = \mathbb{F}_q$ and ψ be the q^{th}-power Frobenius map. Then $\psi(O) = O$. Recall that $\frac{X}{Y}$ is a uniformizer at O. So $\mathrm{ord}_P\left(\frac{X}{Y} \circ \psi\right) = \mathrm{ord}_P\left(\left(\frac{X}{Y}\right)^q\right) = q$, i.e $e_\psi = q$. Thus ψ is ramified.

By Proposition 2.2.8, we have $\deg \psi = \sum_{P \in \psi^{-1}(Q)} e_\psi(P)$ for any $Q \in E$ and $\psi \in \mathrm{End}(E)$. Take $Q = O$, then we have proved the following proposition

Proposition 3.2.6. Let ψ be an isogeny of an elliptic curve. Then

$$\deg \psi = e_\psi |\ker \psi|.$$

Theorem 3.2.7. Let $\phi \in \mathrm{End}(E)$.

a. For all $Q \in E, |\phi^{-1}(Q)| = \deg_s \phi$. Furthermore, $\deg_i \phi = e_\phi$.

b. If ϕ is unramified, then $|\ker \phi| = \deg \phi$.

c. $\ker \phi \to \mathrm{Aut}(\bar{K}(E)/\phi^*\bar{K}(E))$ via the map $P \mapsto \tau_P^*$ is an isomorphism of groups.

Proof. a) From Proposition 2.2.8, we know that $|\phi^{-1}(Q)| = \deg_s(\phi)$ for almost all $Q \in E$. For any P, P', choose $R \in E$ such that $\phi(R) = P' - P$. Then there is a 1-1 correspondence between the sets $\phi^{-1}(P)$ and $\phi^{-1}(P')$. We claim that $S \mapsto S + R$ give one such bijection. This is because if $S + R = S' + R$, then $S = S'$. On the other hand, given $Q \in \phi^{-1}(P')$, then $\phi(Q) = P' = \phi(R) + P \Rightarrow Q - R \in \phi^{-1}(P)$. This verifies that the map is bijective. So $|\phi^{-1}(Q)|$ is independent of Q and the first part follows. Recall that $\deg \phi = (\deg_i \phi)(\deg_s \phi)$. Set $Q = O$ in (a) so that $|\ker \phi| = \deg_s \phi$. By Proposition 3.2.6, the other part follows.

b) Use the fact that $e_\phi = 1$ and Proposition 3.2.6.

c) For $P \in \ker \phi$ and any $f \in \bar{K}(E)$, we have

$$\tau_P^*(\phi^*(f)) = (\tau_P^* \circ \phi^*)(f) = (\phi \circ \tau_P)^*(f) = \phi^*(f),$$

i.e $\tau_P^* \in \mathrm{Aut}(\bar{K}(E)/\phi^*\bar{K}(E))$. Thus the map is well defined. Since

$$\tau_{P+Q}^* = (\tau_P \circ \tau_Q)^* = (\tau_Q \circ \tau_P)^* = \tau_P^* \circ \tau_Q^*,$$

we note that the map is a homomorphism. Since $|\mathrm{Aut}(\bar{K}(E)/\phi^*\bar{K}(E))| \leq \deg_s \phi$, the proof will be complete if we show that the map is injective. Let $\tau_P^*(f) = f$ for all $f \in \bar{K}(E)$. So $f(P+T) = f(T)$ for all $T \in E$ and $f \in \bar{K}(E)$. In particular, $f(P) = f(O)$ for all $f \in \bar{K}(E)$ so that $P = O$. □

For $\phi \in \mathrm{End}(E)$, recall that ϕ^* on $K(E)$ is given as $f \mapsto f \circ \phi$. On the divisor group, we define $\phi^* : \mathrm{Div}(E) \to \mathrm{Div}(E)$ by $(Q) \mapsto \sum_{P \in \phi^{-1}(Q)} e_\phi(P)(P)$ which $\mathbb{Z}$-linearly extends to the whole divisor. The following proposition provides a method for computing divisors of composition of functions.

Proposition 3.2.8. Let ϕ be a non-constant rational map on E. Then the following diagram commutes

$$\begin{array}{ccc} K(E) & \xrightarrow{\phi^*} & K(E) \\ \Big\downarrow \text{div} & & \Big\downarrow \text{div} \\ \text{Div}(E) & \xrightarrow{\phi^*} & \text{Div}(E) \end{array}$$

Proof. We have $\text{div}(\phi^*(f)) = \text{div}(f \circ \phi)$. So

$$\begin{aligned} \text{div}(f \circ \phi) &= \sum_{P \in E} \text{ord}_P(f \circ \phi)(P) = \sum_{P \in E} e_\phi(P) \text{ord}_{\phi(P)}(f)(P) \\ &= \sum_{P \in E} \text{ord}_{\phi(P)}(f) e_\phi(P)(P) = \sum_{R \in E} \text{ord}_R(f) \sum_{P \in \phi^{-1}(R)} e_\phi(P)(P) \\ &= \sum_{R \in E} \text{ord}_R(f) \phi^*((R)) = \phi^* \left(\sum_{R \in E} \text{ord}_R(f)(R) \right) \\ &= \phi^*(\text{div}(f)). \end{aligned}$$

□

Proposition 3.2.9. The endomorphism ring $\text{End}(E)$ is a torsion-free $\mathbb{Z}$ module and has no zero divisors.

Proof. Suppose ψ is a non-constant torsion element of order m. Then $[m] \circ \psi = [0]$. Taking degrees both sides yields $(\deg [m])(\deg \psi) = 0$ which is a contradiction. This proves the first part. For the second part, consider $\psi \circ \phi = [0]$. As before, take degrees so that $(\deg \psi)(\deg \phi) = 0$. Hence, one of the isogenies must be the zero map. □

Definition 3.2.10. For an elliptic curve E, the m-torsion subgroup denoted by $E[m]$ is defined by

$$E[m] = \{P \in E : mP = O\}$$

and the torsion subgroup of E is the set $E_{\text{tors}} = \bigcup_{m=1}^{\infty} E[m]$. For E/K, we use the notation $E_{\text{tors}}(K)$ to mean points of finite order in $E(K)$. Unless otherwise specified, we shall write ω for a non-zero invariant differential on E.

Theorem 3.2.11. Let $\psi, \phi : E \to E'$ be isogenies. Then $(\psi + \phi)^*\omega = \psi^*\omega + \phi^*\omega$.

Proof. See [8]. □

Corollary 3.2.12. For $m \in \mathbb{Z}$, we have $[m]^*\omega = m\omega$

Proof. Clearly for $m = 0$ and $m = 1$, the result holds. For $m = -1$, note that $[-1](x, y) = (x, -y - a_1x - a_3)$ so that

$$[-1]^*\omega = [-1]^*\left(\frac{dx}{2y + a_1x + a_3}\right) = \frac{dx}{2(-y - a_1x - a_3) + a_1x + a_3} = -\frac{dx}{2y + a_1x + a_3}.$$

Since $[m+1]^*\omega = [m]^*\omega + [1]^*\omega$ by Theorem 3.2.11, the rest proceeds by induction on m (downwards and upwards). □

Corollary 3.2.13. A non-constant multiplication-by-m map $[m]$ on E is separable.

Proof. We note that $[m]^*\omega = m\omega \neq 0$ which means that $[m]$ is separable by Proposition 2.3.7 (c). □

Corollary 3.2.14. Let E be defined over a finite field $\mathbb{F}_q$ with characteristic p. Let $\psi : E \to E$ be the q^{th}-power Frobenius morphism. For $m, n \in \mathbb{Z}$, the map $[m]+[n]\psi : E \to E$ is inseparable if and only if $p|m$.

Proof. By Example 3.2.5, we know that ψ is ramified therefore inseparable. So $([m] + [n] \circ \psi)^*\omega = m\omega = 0$ if and only if $p|m$. □

We will use the following proposition to show that for an elliptic curve defined over a characteristic zero field, its endomorphism ring is commutative.

Proposition 3.2.15. Let E/K be an elliptic curve and $\phi \in \mathrm{End}(E)$. Then $\mathrm{div}(\phi^*\omega) = \phi^*\mathrm{div}(\omega)$ and $\mathrm{div}(\omega) = 0$.

Proof. See [8]. □

Theorem 3.2.16. Consider an elliptic curve E/K. Let $\nu : \mathrm{End}(E) \to \bar{K}$ be defined by $\phi \mapsto c_\phi$ where $\phi^*\omega = c_\phi\omega$. Then

a. ν is a homomorphism of rings.

b. $\ker \nu$ consists of inseparable endomorphisms.

Proof. a) Recall that $\dim_{\bar{K}(E)}\Omega_E = 1 \Rightarrow \phi^*\omega = c_\phi\omega$ for some $c_\phi \in \bar{K}(E)$. Furthermore, we have

$$\operatorname{div}(\phi^*\omega) = \operatorname{div}(c_\phi\omega) = \operatorname{div}(c_\phi) + \operatorname{div}(\omega) = \operatorname{div}(c_\phi) = 0.$$

This follows from Proposition 3.2.15. Thus $\operatorname{div}(c_\phi) = 0$ implies that c_ϕ has no poles or zeros, hence $c_\phi \in \bar{K}$. So ν is well defined. By Theorem 3.2.11, it follows that

$$c_{\phi+\psi}\omega = (\phi+\psi)^*\omega = \phi^*\omega + \psi^*\omega = c_\phi\omega + c_\psi\omega$$

so that $\nu(\phi+\psi) = \nu(\phi) + \nu(\psi)$.

b) We know that $c_\phi = 0$ is the same as $\phi^*\omega = 0$ which is the same as saying ϕ is inseparable.

□

Consequently, if $\operatorname{char} K = 0$, then every non-constant endomorphism is separable, and so $\operatorname{End}(E) \hookrightarrow \bar{K}$ which implies that $\operatorname{End}(E)$ is commutative. This result will be helpful in the characterisation of $\operatorname{End}(E)$.

Let $\psi : E \to E'$ be a non-constant isogeny of degree m. There is a unique isogeny denoted $\widehat{\psi} : E' \to E$ satisfying $\widehat{\psi} \circ \psi = [m]$, see [8]. Now suppose that $\widehat{\psi}_1 \circ \psi = \widehat{\psi}_2 \circ \psi$. Then $(\widehat{\psi}_1 - \widehat{\psi}_2) \circ \psi = [0]$. Since ψ is non-constant, it follows that $\widehat{\psi}_1 = \widehat{\psi}_2$. We call $\widehat{\psi}$, the *dual isogeny*. If $\psi = [0]$, we set $\widehat{\psi} = [0]$.

Theorem 3.2.17. With the notation above, we have the following

a. $\psi \circ \widehat{\psi} = [m]_{E'}$ where $[m]_{E'}$ denotes $[m]$ on E'.

b. Let $\lambda : E' \to E''$ be another isogeny with $\deg\lambda = n$. Then $\widehat{\lambda \circ \psi} = \widehat{\psi} \circ \widehat{\lambda}$.

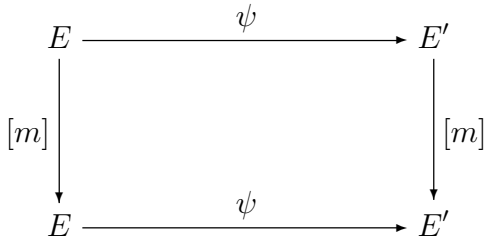
c. If ϕ is another isogeny from E to E', then $\widehat{\psi + \phi} = \widehat{\psi} + \widehat{\phi}$.

d. For all $m \in \mathbb{Z}$, $\widehat{[m]} = [m]$ and $\deg[m] = m^2$.

e. $\deg\widehat{\psi} = \deg\psi$.

f. $\widehat{\widehat{\psi}} = \psi$.

Proof. a) Since ψ is a homomorphism, the following diagram commutes:



Hence $\psi \circ [m]_E = [m]_{E'} \circ \psi \Rightarrow \psi \circ (\widehat{\psi} \circ \psi) = [m]_{E'} \circ \psi \Rightarrow \psi \circ \widehat{\psi} = [m]_{E'}$.

b) $(\widehat{\psi} \circ \widehat{\lambda})(\lambda \circ \psi) = \widehat{\psi} \circ (\widehat{\lambda} \circ \lambda) \circ \psi = \widehat{\psi} \circ [n]_{E'} \circ \psi = (\widehat{\psi} \circ \psi) \circ [n]_E = [m]_E \circ [n]_E = [mn]$. On the other hand, we have $(\widehat{\psi \circ \lambda})(\lambda \circ \psi) = [mn]$ and thus applying uniqueness of $\widehat{\lambda \circ \psi}$ yields the result.

c) Refer to [8].

d) The first part is clearly true for $m = 0, 1$. By induction on $m \geq 0$, $\widehat{[m+1]} = \widehat{[m]} + \widehat{[1]} = [m+1]$. For downward induction ($m < 0$), we use the fact that $\widehat{[-1]} = [-1]$. Say $m = -k$ where $k > 0$. We have $\widehat{[-k]} = \widehat{[k]} \circ \widehat{[-1]} = [k][-1] = [-k] = [m]$. For the second part, note that $[m]\widehat{[m]} = [m^2] \Rightarrow \deg [m] = m^2$.

e) We have $[m^2] = [\deg [m]] = [\deg \widehat{\psi} \circ \psi] = [\deg \widehat{\psi} \deg \psi] = [m \deg \widehat{\psi}] \Rightarrow \deg \widehat{\psi} = m = \deg \psi$.

f) Clearly $\widehat{\psi} \circ \psi = [m] = \widehat{[m]} = \widehat{\widehat{\psi} \circ \psi} = \widehat{\psi} \circ \widehat{\widehat{\psi}}$ and the result follows from uniqueness of $\widehat{\psi}$. □

Proposition 3.2.18. Let $p = \text{char } K$.

a. If $p > 0$, then either of the following is true but not both

   i. $E[p^r] = \{O\}$ for all $r = 1, 2, \ldots$.

   ii. $E[p^r] \cong \mathbb{Z}/p^r\mathbb{Z}$ for all $r = 1, 2, \ldots$.

b. If $p = 0$ or p does not divide m, then $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

Proof. a) Let ϕ be the p^{th}-power Frobenius morphism. Note that $|E[p^r]| = \deg_s [p^r] = (\deg_s \widehat{\phi} \circ \phi)^r$ by Theorems 3.2.7 and 3.2.17 (a). Recall that $\deg \phi = p$. Since ϕ is inseparable, we have $\deg_s \phi = 1 \Rightarrow |E[p^r]| = (\deg \widehat{\phi})^r$. If $\widehat{\phi}$ is inseparable, then $\deg_s \widehat{\phi} = 1 \Rightarrow |E[p^r]| = \{O\}$ for all $r = 1, 2, \ldots$. Otherwise, $\deg_s \widehat{\phi} = p$ so that $|E[p^r]| = p^r$. We will show that $E[p^r]$ is cyclic.

For $r = 1$, clearly $E[p] \cong \mathbb{Z}/p\mathbb{Z}$. Assume by induction that $E[p^{r-1}] \cong \mathbb{Z}/p^{r-1}\mathbb{Z}$. Define $\eta : E[p^r] \to E[p^{r-1}]$ by $P \mapsto pP$. We note that η is the restriction of the surjective map $[p]$ on $E[p^r]$. Clearly, the preimage of a p^{r-1}-torsion point under $[p]$ is a p^r-torsion point. Hence η is a surjective homomorphism. By the induction hypothesis, there is $Q \in E[p^{r-1}]$ which has order p^{r-1}. So there is $P \in E[p^r]$ such that $pP = Q$. But $p^{r-1}Q = O$ and $p^iQ \neq O$ for all $1 \leq i \leq r-2$ implies that P has order p^r.

b) We know that $|E[m]| = m^2$. Suppose m is prime. Then by the fundamental theorem on finite abelian groups, $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ or $E[m] \cong \mathbb{Z}/m^2\mathbb{Z}$. But the later case means that $E[m]$ contains a point of order m^2 which is not annihilated upon multiplication by m, a contradiction.

Suppose m is not prime, then $m = m'q$ with q a prime. We then have

$$\begin{aligned} E[m'] &= \{P : m'P = O\} \\ &= \{qP : m'qP = O\} \text{ since } [q] \text{ is surjective} \\ &= \{qP : mP = O\} = qE[m]. \end{aligned}$$

Again by the fundamental theorem, we have

$$E[m] \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \ldots \times \mathbb{Z}/n_r\mathbb{Z}$$

with unique $n_1, n_2, \ldots, n_r \geq 2$ such that $n_i | n_{i+1}$. Hence $E[m'] \cong q\mathbb{Z}/n_1\mathbb{Z} \times q\mathbb{Z}/n_2\mathbb{Z} \times \ldots \times q\mathbb{Z}/n_r\mathbb{Z} \cong \mathbb{Z}/s_1\mathbb{Z} \times \mathbb{Z}/s_2\mathbb{Z} \times \ldots \times \mathbb{Z}/s_r\mathbb{Z}$ where

$$s_i = \begin{cases} n_i & \text{if } q \text{ does not divide } n_i \\ \frac{n_i}{q} & \text{if } q \text{ divides } n_i \end{cases}$$

and s_i divides s_{i+1} since $n_i | n_{i+1}$. By induction hypothesis to m', i.e $E[m'] \cong \mathbb{Z}/m'\mathbb{Z} \times \mathbb{Z}/m'\mathbb{Z}$ and the fact that s_i's are unique, we have $s_1 = s_2 = \ldots = s_{r-2} = 1$ and $s_{r-1} = s_r = m'$. Hence $n_1 = n_2 = \ldots = n_{r-2} = q$ and $n_{r-1} = n_r = qm' = m$. So $|E[m]| = m^2 = q^{r-2}m^2 \Rightarrow r = 2$. □

Lemma 3.2.19. Let $m, n \in \mathbb{Z}$ and $(m, n) = 1$. Then $E[mn] \cong E[m] \times E[n]$.

Proof. There are integers x_1 and x_2 such that $x_1n + x_2m = 1$. Define maps $\pi : E[m] \times E[n] \to E[mn]$ by $(P, Q) \mapsto P+Q$ and $\pi' : E[mn] \to E[m] \times E[n]$ by $P \mapsto (x_1nP, x_2mP)$. It is not difficult to see that the two maps are inverse group isomorphisms. □

Theorem 3.2.20. With the notation introduced in Proposition 3.2.18, if p divides m, then

$$E[m] \cong \mathbb{Z}/m'\mathbb{Z} \times \mathbb{Z}/m'\mathbb{Z} \text{ or } E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m'\mathbb{Z}$$

where $m = p^n m'$ with $(m', p) = 1$.

Proof. By Lemma 3.2.19, $E[m] \cong E[m'] \times E[p^n]$. If $E[p] = \{O\}$, then $E[p^n] = \{O\}$ by Proposition 3.2.18(a). So $E[m] \cong \mathbb{Z}/m'\mathbb{Z} \times \mathbb{Z}m'/\mathbb{Z}$. On the other hand, if $E[p^n] = \mathbb{Z}/p^n\mathbb{Z}$, then $E[m] \cong E[m'] \times \mathbb{Z}/p^n\mathbb{Z} \cong \mathbb{Z}/m'\mathbb{Z} \times \mathbb{Z}/m'\mathbb{Z} \times \mathbb{Z}/p^n\mathbb{Z}$. Since $\mathbb{Z}/m'\mathbb{Z} \times \mathbb{Z}/p^n\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z}$ by Chinese Remainder Theorem, we have $E[m] \cong \mathbb{Z}/m'\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. □

We call an elliptic curve in finite characteristic p *ordinary* if $E[p] \cong \mathbb{Z}/p\mathbb{Z}$ and *supersingular* if $E[p] \cong 0$.

3.3 Weil pairing and elliptic curves over finite fields

The Weil pairing will be indirectly important in computing the cardinality of torsion points on elliptic curves defined over finite fields. We exhibit its construction and deduce its properties.

Assume E is defined over K and $(\operatorname{char} K, m) = 1$. Let $T \in E[m]$. The divisor $m(T) - m(O)$ is principal by Proposition 3.1.3. So there is $f \in K(E)^\times$ such that $\operatorname{div}(f) = m(T) - m(O)$. Let $T' \in E[m^2]$ be chosen such that $mT' = T$. Then the divisor $\sum_{S \in E[m]}(T' + S) - (S)$ is principal since $\sum_{S \in E[m]} T' + S - S = m^2T' = O$ and the degree of the divisor is 0. So we can find a function g such that $\operatorname{div}(g) = \sum_{S \in E[m]}(T' + S) - (S)$. Let $\tilde{T} = T' + S$ in the summation. Clearly $\tilde{T} = T' + S \Leftrightarrow m\tilde{T} = mT' + mS = T$. Hence we can restate the divisor of g as

$$\operatorname{div}(g) = \sum_{m\tilde{T}=T} (\tilde{T}) - \sum_{mS=O} (S).$$

We want to compute $\operatorname{div}(f \circ m)$. We know that $[m]$ is separable and $e_{[m]}(P) = 1$ for all $P \in E$. By definition, we have

$$\begin{aligned}\operatorname{div}(f \circ m) = [m]^* (\operatorname{div}(f)) &= m \sum_{P \in [m]^{-1}(T)} e_{[m]}(P)(P) - m \sum_{Q \in [m]^{-1}(O)} e_{[m]}(Q)(Q) \\ &= m \sum_{mP=T} (P) - m \sum_{mQ=O} (Q) \\ &= \operatorname{div}(g^m).\end{aligned}$$

It follows that $f \circ g = k g^m$ for some $k \in \bar{K}$. Without loss of generality, assume $k = 1$. Then for $S \in E[m]$ and $P \in E$, we have $g(P+S)^m = f(m(P+S)) = f(mP) = g(P)^m \Rightarrow \frac{g(P+S)}{g(P)}$ is an m^{th} root of unity. Let $\mu_m = \{x \in \bar{K} : x^m = 1\}$.

Definition 3.3.1. The m^{th} Weil pairing is the map $e_m : E[m] \times E[m] \to \mu_m$ defined by

$$e_m(S, T) = \frac{g(P + S)}{g(P)}$$

where P is any point on E such that $g(P + S)$ and $g(P)$ are defined and nonzero.

Maintaining our assumption on m, we have the following theorem.

Theorem 3.3.2. The map e_m satisfies the following properties

a. Bilinearity in each variable, i.e $e_m(S_1 + S_2, T) = e_m(S_1, T) e_m(S_2, T)$ and $e_m(S, T_1 + T_2) = e_m(S, T_1) e_m(S, T_2)$ for all $S, T, S_1, S_2, T_1, T_2 \in E[m]$.

b. $e_m(T, T) = 1$ for all $T \in E[m]$ and so $e_m(S, T) = e_m(T, S)^{-1}$ for all $S, T \in E[m]$.

c. Nondegeneracy in both variables, i.e $e_m(S, T) = 1$ for all $T \in E[m] \Rightarrow S = O$ and $e_m(S, T) = 1$ for all $S \in E[m] \Rightarrow T = O$.

d. $e_m(\sigma S, \sigma T) = \sigma e_m(S, T)$ for all $\sigma \in \operatorname{Gal}(\bar{K}/K)$.

e. $e_m(\alpha(S), \alpha(T)) = e_m(S, T)^{\deg \alpha}$ for all endomorphisms α.

Proof. (a) $e_m(S_1 + S_2, T) = \frac{g(P+S_1+S_2)}{g(P)} = \frac{g(P+S_1+S_2)}{g(P+S_1)} \frac{g(P+S_1)}{g(P)} = e_m(S_2, T) e_m(S_1, T)$. For the second part, let $T_3 = T_1 + T_2$. Then there is $\tilde{g} \in K(E)^\times$ such that

$$\operatorname{div}(\tilde{g}) = (T_1) + (T_2) - (T_3) - (O).$$

Let f_i, g_i be the functions used to define $e_m(S, T_i)$. Thus $\operatorname{div}(f_i) = m(T_i) - m(O)$ and $g_i^m = f_i \circ m$. We have

$$\begin{aligned}\operatorname{div}\left(\frac{f_3}{f_1 f_2}\right) &= \operatorname{div}(f_3) - \operatorname{div}(f_1) - \operatorname{div}(f_3) \\ &= m(T_3) - m(O) - m(T_2) + m(O) - m(T_1) + m(O) \\ &= m(\operatorname{div}(\tilde{g})) = \operatorname{div}(\tilde{g}^m)\end{aligned}$$

implying that $\frac{f_3}{f_1 f_2} = b\tilde{g}^m$ for some $b \in \bar{K}^\times \Rightarrow f_3 = b f_1 f_2 \tilde{g}^m$. Composing with m, we get $f_3 \circ m = b(f_1 \circ m)(f_2 \circ m)(\tilde{g}^m \circ m) \Rightarrow g_3^m = b g_1^m g_2^m (\tilde{g} \circ m)^m \Rightarrow g_3 = b^{1/m} g_1 g_2 (\tilde{g} \circ m)$ so that

$$\begin{aligned}e_m(S, T_1 + T_2) = \frac{g_3(P+S)}{g_3(P)} &= \frac{g_1(P+S)}{g_1(P)} \frac{g_2(P+S)}{g_2(P)} \frac{\tilde{g}(mP+O)}{\tilde{g}(mP)} \\ &= e_m(S, T_1) e_m(S, T_2)\end{aligned}$$

(b) Recall the translation by Q map written τ_Q. Now for $j \in \mathbb{Z}_{\geq 0}$, we note the following

$$\begin{aligned}\operatorname{div}(f \circ \tau_{jT}) &= \tau_{jT}^*(\operatorname{div}(f)) \\ &= m \sum_{P \in \tau_{jT}^{-1}(T)} (P) - m \sum_{Q \in \tau_{jT}^{-1}(O)} (O) \text{ since } e_{\tau_{jT}}(P) = 1 \text{ for all } P \in E \\ &= m(T - jT) - m(-jT)\end{aligned}$$

which implies

$$\operatorname{div} \prod_{j=0}^{m-1} f \circ \tau_{jT} = \sum_{j=0}^{m-1} m(T - jT) - m(-jT) = 0,$$

and so $\prod_{j=0}^{m-1} f \circ \tau_{jT} \in \bar{K}$. Recall that $mT' = T$. We deduce that

$$\begin{aligned}\left(\operatorname{div} \prod_{j=0}^{m-1} g \circ \tau_{jT'}\right)^m &= \operatorname{div} \prod_{j=0}^{m-1} g^m \circ \tau_{jT'} \\ &= \operatorname{div} \prod_{j=0}^{m-1} f \circ [m] \circ \tau_{jT'} \\ &= \operatorname{div} \prod_{j=0}^{m-1} f \circ \tau_{jT} \circ [m].\end{aligned}$$

The last statement follows from the fact that

$$[m] \circ \tau_{jT'}(P) = m(P + jT') = mP + jmT'$$

which is equal to

$$mP + jT = ([m] \circ \tau_{jT})(P) = (\tau_{jT} \circ [m])(P).$$

Clearly $\prod_{j=0}^{m-1} f \circ \tau_{jT} \circ [m]$ is constant and so $\prod_{j=0}^{m-1} g \circ \tau_{jT'}$ is constant. Hence at P and $P + T'$, the product takes the same value, i.e

$$\prod_{j=0}^{m-1} g \circ \tau_{jT'}(P) = \prod_{j=0}^{m-1} g \circ \tau_{jT'}(P + T')$$

which implies that

$$g(P) = g(P + mT') = g(P + T) \Rightarrow \frac{g(P+T)}{g(P)} = e_m(T, T) = 1.$$

Using bilinearity, we have

$$e_m(S + T, S + T) = e_m(S, T)e_m(T, S)e_m(S, S)e_m(T, T)$$

which implies that $e_m(S, T) = e_m(T, S)^{-1}$.

(c.) Let $T \in E[m]$ such that $e_m(S, T) = 1$ for all $S \in E[m]$. Then $g(S + P) = g(P)$ for all $S \in E[m]$. In other words, $(g \circ \tau_S) = \tau_S^*(g) = g$ for all $S \in E[m]$. By Theorem 3.2.7, we have $g \in \mathrm{Aut}(K(E)/[m]^*\bar{K}(E))$ which implies that $g = \tilde{f} \circ [m]$ for some $\tilde{f} \in \bar{K}(E)$. Now

$$\tilde{f}^m \circ [m] = g^m = f \circ [m] \Rightarrow f = \tilde{f}^m$$

since $[m]$ is a non-constant map. We have

$$m\mathrm{div}(\tilde{f}) = \mathrm{div}(f) = m(T) - m(O) \Rightarrow \mathrm{div}(\tilde{f}) = (T) - (O)$$

so that $T = O$ by Proposition 2.3.13. On the other hand, if $S \in E[m]$ such that $e_m(S, T) = 1$ for all $T \in E[m]$, then $e_m(T, S) = 1$ for all $T \Rightarrow S = O$.

(d.) Consider the functions f and g in our construction. Then

$$\mathrm{div}(f^\sigma) = m(\sigma(T)) - m(\sigma(O)) = m(\sigma(T)) - m(O)$$

and

$$\sigma(e_m(S, T)) = \frac{g^\sigma(\sigma(P) + \sigma(T))}{g^\sigma(\sigma(P))} = e_m(\sigma(S), \sigma(T)).$$

(e.) Let α be a separable endomorphism and $\ker\alpha = \{B_1, B_2, \ldots, B_s\}$. Thus $\deg\alpha = s$. Let $\operatorname{div}(f_T) = m(T) - m(O)$ and $\operatorname{div}(f_{\alpha(T)}) = m(\alpha(T)) - m(O)$ and we have $f_T \circ [m] = g_T^m$ and $f_{\alpha(T)} \circ [m] = g_{\alpha(T)}^m$. Let τ_B be the translation by B. We note that

$$\operatorname{div}(f_T \circ \tau_{-B_i}) = \tau_{-B_i}^*(\operatorname{div}(f_T)) = m(T + B_i) - m(B_i)$$

and

$$\begin{aligned}
\operatorname{div}(f_{\alpha(T)} \circ \alpha) &= m \sum_{Q \in \alpha^{-1}(\alpha(T))} (Q) - m \sum_{R \in \alpha^{-1}(O)} (R) \\
&= m \sum_{\alpha(Q) = \alpha(T)} (Q) - m \sum_{\alpha(R) = O} (R) \\
&= m \left(\sum_i (T + B_i) - m(B_i) \right) \\
&= \operatorname{div} \left(\prod_i f_T \circ \tau_{-B_i} \right).
\end{aligned}$$

Applying the same trick as before, for every i, choose B_i' such that $mB_i' = B_i$. Then a calculation shows that $g_T(P - B_i')^m = f_T(mP - B_i)$ and hence

$$\begin{aligned}
\operatorname{div} \left(\prod_i (g_T \circ \tau_{-B_i'})^m \right) &= \operatorname{div} \prod_i f_T \circ [m] \circ \tau_{-B_i} \\
&= \operatorname{div} \prod_i f_T \circ \tau_{-B_i} \circ [m] \\
&= [m]^* \operatorname{div} \left(\prod_i f_T \circ \tau_{-B_i} \right) \\
&= [m]^* \operatorname{div}(f_{\alpha(T)} \circ \alpha) \\
&= \operatorname{div}(f_{\alpha(T)} \circ \alpha \circ [m]) \\
&= \operatorname{div}(g_{\alpha(T)}^m \circ \alpha) \\
&= \operatorname{div}(g_{\alpha(T)} \circ \alpha)^m
\end{aligned}$$

which implies that

$$\prod_i (g_T \circ \tau_{-B_i'}) = c g_{\alpha(T)} \circ \alpha \text{ for some } c \in \bar{K}. \tag{3.3.1}$$

So we have

$$\begin{aligned} e_m(\alpha(S),\alpha(T)) &= \frac{g_{\alpha(T)}(\alpha(P)+\alpha(S))}{g_{\alpha(T)}\alpha(P)} \\ &= \frac{(g_{\alpha(T)}\circ\alpha)(P+S)}{(g_{\alpha(T)}\circ\alpha)(P)} \\ &= \frac{\prod_i g_T(P-B_i'+S)}{g_T(P-B_i')} \text{ by Equation 3.3.1} \\ &= \prod_i e_m(S,T) \text{ by definition of } e_m \\ &= e_m(S,T)^{\deg\alpha}. \end{aligned}$$

For α inseparable, refer to [10].

□

From $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, we note that $E[m]$ is a $\mathbb{Z}/m\mathbb{Z}$-module of rank 2. So we can find 2 linearly independent generators T_1 and T_2 for $E[m]$. For an endomorphism α, we have $\alpha(T_1) = aT_1 + cT_2$ and $\alpha(T_2) = bT_1 + dT_2$ for some $a, b, c, d \in \mathbb{Z}/m\mathbb{Z}$. We define α_m to be the matrix

$$\alpha_m = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Corollary 3.3.3. Let $\{T_1, T_2\}$ be a basis for $E[m]$. Then $e_m(T_1, T_2)$ is a primitive m^{th} root of unity.

Proof. Let $\gamma = e_m(T_1, T_2)$ with $\gamma^n = 1$. Then by bilinearity, we have $e_m(T_1, nT_2) = 1$ and $e_m(T_2, nT_2) = 1$. Let $P \in E[m]$. Then $P = aT_1 + bT_2$ for some $a, b \in \mathbb{Z}$. So $e_m(P, nT_2) = e_m(aT_1 + bT_2, nT_2) = e_m(T_1, nT_2)^a e_m(T_2, nT_2)^b = e_m(T_1, T_2)^{an} e_m(T_2, T_2)^{nb} = 1$, i.e $e_m(P, nT_2) = 1$ for all $P \in E[m] \Rightarrow nT_2 = O \Leftrightarrow m|n \Rightarrow \gamma$ is a primitive m^{th} root of unity. □

Corollary 3.3.4. If $E[m] \subseteq E(K)$, then $\mu_m \in K$.

Proof. As before, let $\{T_1, T_2\}$ be a basis for $E[m]$. By assumption, $\sigma(T_i) = T_i$ for all $\sigma \in \text{Gal}(\bar{K}/K)$ and $i = 1, 2$. Now $\gamma = e_m(\sigma(T_1), \sigma(T_2))) = \sigma(e_m(T_1, T_2)) = \sigma(\gamma)$ so that $\gamma \in K$. By Corollary 3.3.3, γ generates μ_m and so $\mu_m \subset K$. □

One of the applications of Corollary 3.3.4 is that $E[m] \nsubseteq E(\mathbb{Q})$ for all $m \geq 3$. To see this, assume that $E[m] \subseteq E(\mathbb{Q})$ for some $m \geq 3$ then $\mu_m \in \mathbb{Q}$, which is a contradiction.

Proposition 3.3.5. Let E be defined over K and $\alpha \in \mathrm{End}(E)$. Assume $(\mathrm{char}\, K, m) = 1$. Then

$$\det \alpha_m \equiv \deg \alpha \pmod{m}.$$

Proof. Maintaining the notation in Corollary 3.3.3, we note that $\gamma^{\deg \alpha} = e_m(T_1, T_2)^{\deg \alpha} = e_m(\alpha(T_1), \alpha(T_2)) = e_m(aT_1 + cT_2, bT_1 + dT_2) = e_m(T_1, T_2)^{ad-bc} = \gamma^{\det \alpha_m}$, and the result follows. □

Proposition 3.3.6. Let α be a non-zero endomorphism. Then $\alpha^2 - [1 + \deg \alpha - \deg([1] - \alpha)]\alpha + \deg \alpha = [0]$.

Proof. Let $f = \alpha^2 - [1 + \deg \alpha - \deg([1] - \alpha)]\alpha + \deg \alpha$. Restricting all the endomorphisms to $E[m]$ for $(m, \mathrm{char}\, K) = 1$, we have $f_m = \alpha_m^2 - [1 + \det \alpha_m - \det(\mathrm{I} - \alpha_m)]\alpha_m + \det \alpha_m$. Clearly $\mathrm{Tr}\, \alpha_m = 1 + \det \alpha_m - \det(\mathrm{I} - \alpha_m)$, and so by Cayley-Hamilton theorem, $f_m = 0$. Varying m, we note that $f(P) = O$ for infinitely many torsion points P. It follows that $f(P) = O$ for all P on E, otherwise we would have $f = (\psi, \phi)$ where ϕ or ψ has infinitely many poles, which is a contradiction. □

3.3.7 Elliptic curves over a finite field

In this section we look at elliptic curves over $\mathbb{F}_q$ with characteristic $p > 0$. One of the tasks is to derive a formula for computing the number of points on an elliptic curve with coordinates in higher extensions of $\mathbb{F}_q$. We first begin with an estimate on the number of points on $E(\mathbb{F}_q)$.

3.3.8 Hasse's Theorem

Definition 3.3.9. Let $\mathcal{G}$ be an abelian group. A function $q : \mathcal{G} \to \mathbb{R}$ is called positive definite quadratic form if it satisfies the following

a. $q(-a) = q(a)\ \forall\ a \in \mathcal{G}$.

b. $q(a) \geq 0\ \forall\ a \in \mathcal{G}$.

c. $q(a) = 0$ if and only if $a = 0$.

d. The map $(a, b) \mapsto q(a + b) - q(a) - q(b)$ is bilinear.

Lemma 3.3.10. The degree map $\deg : \mathrm{Hom}(E, E') \to \mathbb{Z}$ is a positive definite quadratic form.

Proof. a) Note that $-\phi = [-1]_{E'} \circ \phi \Rightarrow \deg(-\phi) = \deg[-1]_{E'} \deg\phi = \deg\phi$

b) Let $\langle\phi, \psi\rangle = \deg(\phi + \psi) - \deg\phi - \deg\psi$. Then

$$\begin{aligned}
[\langle\phi, \psi\rangle]_E &= [\deg(\phi + \psi)]_E - [\deg\phi]_E - [\deg\psi]_E \\
&= \widehat{(\phi + \psi)} \circ (\phi + \psi) - \widehat{\phi} \circ \phi - \widehat{\psi} \circ \psi \\
&= (\widehat{\phi} + \widehat{\psi}) \circ (\phi + \psi) - \widehat{\phi} \circ \phi - \widehat{\psi} \circ \psi \\
&= \widehat{\phi} \circ \psi + \widehat{\psi} \circ \phi.
\end{aligned}$$

From this, it follows that for all $\phi_1, \phi_2 \in \mathrm{Hom}(E, E')$,

$$[\langle\phi_1 + \phi_2, \psi\rangle]_E = [\langle\phi_1, \psi\rangle]_E + [\langle\phi_2, \psi\rangle]_E = [\langle\phi_1, \psi\rangle + \langle\phi_2, \psi\rangle]_E.$$

As $\mathbb{Z}$ injects into $\mathrm{End}(E)$, we must have $\langle\phi_1 + \phi_2, \psi\rangle = \langle\phi_1, \psi\rangle + \langle\phi_2, \psi\rangle$. Linearity in the second variable holds in a similar way.

(c) Clear since $\deg\phi > 0$ for ϕ non-constant. □

Lemma 3.3.11. Let $\mathcal{G}$ be an abelian group and $q : \mathcal{G} \to \mathbb{R}$ a positive definite quadratic form. Then

$$|q(\psi - \phi) - q(\psi) - q(\phi)| \leq 2\sqrt{q(\phi)q(\psi)} \text{ forall } \psi, \phi \in \mathcal{G}$$

Proof. Let $\langle\phi, \psi\rangle = q(\psi+\phi)-q(\psi)-q(\phi)$. Then $\langle-\phi, \phi\rangle = q(0)-q(-\phi)-q(\phi) = -2q(\phi)$ for all $\phi \in \mathcal{G}$. Note that $\langle-m\phi, m\phi\rangle = m^2\langle-\phi, \phi\rangle$, using bilinearity. Thus $\langle-m\phi, m\phi\rangle = -2m^2q(\phi)$ for all $m \in \mathbb{Z}$. On the other hand, $\langle-m\phi, m\phi\rangle = -2q(m\phi)$ by definition. Hence $q(m\phi) = m^2q(\phi)$ for all $m \in \mathbb{Z}$.

If $\psi = 0$, the inequality holds. So we assume that $\psi \neq 0$. Then

$$\begin{aligned}
q(m\psi - n\phi) &= \langle m\psi, -n\phi\rangle + q(m\psi) + q(n\phi) \\
&= -mn\langle\psi, \phi\rangle + m^2q(\psi) + n^2q(\phi) \text{ for any } m, n \in \mathbb{Z}.
\end{aligned}$$

Setting $m = \langle \psi, \phi \rangle$ and $n = 2q(\psi)$, we get $q(m\psi - n\phi) = -q(\psi)\langle \psi, \phi \rangle^2 + 4q(\psi)^2 q(\phi)$. Since q is positive definite, we obtain the inequality, $q(\psi)[4q(\psi)q(\phi) - \langle \psi, \phi \rangle^2] \geq 0$. Now $\psi \neq 0$ implies the result. □

Since the equation of E has coefficients in $\mathbb{F}_q$, it follows that the q^{th}-power Frobenius map is an automorphism. Let ϕ_q represent this map, then $\phi_q : E \to E$ is defined as $(x, y) \mapsto (x^q, y^q)$. Obviously, $P \in E(\mathbb{F}_q)$ if and only if $\phi_q(P) = P$ i.e $P \in \ker(1 - \phi_q)$. By Corollary 3.3.12, $1 - \phi_q$ is separable, and thus $|\ker(1 - \phi_q)| = \deg(1 - \phi_q) = \#E(\mathbb{F}_q)$.

Theorem 3.3.12. (Hasse) Let E be an elliptic curve over a finite field $\mathbb{F}_q$. Then

$$|\#E(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}.$$

Proof. Take $\mathcal{G} = \text{End}(E)$ and $\psi = [1]$ in Lemma 3.3.11 so that

$$|\deg(1 - \phi_q) - 1 - \deg \phi_q| \leq 2\sqrt{\deg \phi_q}.$$

Using the fact that $\deg \phi_q = q$, the result follows. □

Theorem 3.3.13. For $E/\mathbb{F}_q$, let ϕ_q be the q^{th}-power Frobenius map and $a = q + 1 - \#E(\mathbb{F}_q)$. Let α, β be the roots of the polynomial $X^2 - aX + q$. Then $\#E(\mathbb{F}_{q^n}) = q^n + 1 - \alpha^n - \beta^n$ for all $n \geq 1$.

Proof. By Proposition 3.3.6, we must have $\phi_q^2 - [1 + \deg \phi_q - \deg([1] - \phi_q)]\phi_q + \deg \phi_q = [0]$, i.e $\phi_q^2 - [1 + q - |E(\mathbb{F}_q)|]\phi_q + \deg \phi_q = 0$ in $\text{End}(E)$. Let $a = 1 + q - |E(\mathbb{F}_q)|$. Then ϕ_q is a zero in $\text{End}(E)$ of the polynomial $X^2 - aX + q$. Let $L = \mathbb{F}_{q^n}$ which is a degree n finite extension of $\mathbb{F}_q$ and denote the map $(x, y) \mapsto (x^{q^n}, y^{q^n})$ by ϕ_L. The integer s, if it exists, such that $\phi_L^2 + s\phi_L + q^n = 0$ is unique since, if $\phi_L^2 + s'\phi_L + q^n = 0$ for another integer s', then $s\phi_L - s'\phi_L = 0 \Rightarrow s = s'$ by surjectivity of ϕ_L. By this argument, a is the only number satisfying the equation $X^2 - aX + q = 0$ given that ϕ_q is a zero of the associated polynomial. Using $\phi_L = \phi_q^n$ and Proposition 3.3.6, we note that $s = 1 + q^n - |E(\mathbb{F}_{q^n})|$ is the unique integer such that $(\phi_q^n)^2 - s\phi_q^n + q^n = 0$, i.e ϕ_q is a root of the polynomial $X^{2n} - sX^n + q^n$.

Let α and β be roots of the polynomial $X^2 - aX + q$ so that $a = \alpha + \beta$ and $\alpha\beta = q$. Denote the discriminant of the quadratic by D, so $D = a^2 - 4q$. By Theorem 3.3.12,

D is not a positive integer. Clearly, α and β are integers in the imaginary quadratic extension $\mathbb{Q}(\sqrt{D})$, i.e $\alpha, \beta \in \mathbb{Z}[\theta]$ where $\theta = \frac{1+\sqrt{D}}{2}$ if $D \equiv 1 (\text{mod } 4)$ and $\theta = \sqrt{D}$, otherwise. Since $D < 0$, α and β are complex conjugates, and thus $\alpha^n + \beta^n \in \mathbb{R}$. Hence $\alpha^n + \beta^n \in \mathbb{Z}[\theta] \cap \mathbb{R} = \mathbb{Z}$.
Let $g(X) = X^{2n} - (\alpha^n + \beta^n)X^n + q^n$. Then $g(X) \in \mathbb{Z}[X]$. Furthermore, $g(\alpha) = 0$ and $g(\beta) = 0$ so that $X^2 - aX + q$ divides $g(X)$ implying that $\phi_q^{2n} - (\alpha^n + \beta^n)\phi_q^n + q^n = 0$. $\square$

The number a is called the *trace of Frobenius*.

Example 3.3.14. Consider E defined over $\mathbb{F}_2$ given by $y^2 + xy = x^3 + x^2 + 1$. Then $\#E(\mathbb{F}_2) = 2$ so that $a = 2 + 1 - 2 = 1$. Now $\alpha = \frac{1+\sqrt{7}i}{2}$ and $\beta = \frac{1-\sqrt{7}i}{2}$ are the roots of the polynomial $X^2 - X + 2$, and $\alpha^6 + \beta^6 = 9$. By Theorem 3.3.13, $\#E(\mathbb{F}_{2^6}) = 65 - 9 = 56$.

3.4 Characterisation of the endomorphism ring

In this section we would like to characterise the endomorphism ring of an elliptic curve. We do that by proving a general result that applies to certain rings. The tensor product is always taken over $\mathbb{Z}$.

Definition 3.4.1. Let $\mathcal{H}$ be a $\mathbb{Q}$-algebra that is finitely generated over $\mathbb{Q}$. An order in $\mathcal{H}$ is a subring and finitely generated $\mathbb{Z}$-module $\mathcal{R}$ satisfying $\mathcal{R} \otimes \mathbb{Q} = \mathcal{H}$. $\mathcal{R}$ is said to be maximal if given that $\mathcal{R}'$ is an order in $\mathcal{H}$ with $\mathcal{R} \subset \mathcal{R}'$, then $\mathcal{R} = \mathcal{R}'$.

Example 3.4.2. For a quadratic number field $\mathbb{Q}(\sqrt{m})$ where $m < 0$ is square free and 4 does not divide $m - 1$, we note that the ring of integers $\mathbb{Z}[\sqrt{m}]$ is an order since $\mathbb{Z}[\sqrt{m}] \otimes \mathbb{Q} = \mathbb{Q}[\sqrt{m}]$.

Remark 3.4.3. It turns out that an order in an imaginary quadratic extension of $\mathbb{Q}$ can be written in the form $\mathbb{Z} + f\mathcal{R}$ where $f \in \mathbb{Z}_{>0}$ and $\mathcal{R}$ is the ring of integers of the extension. In this case we see that the ring of integers is the maximal order.

Definition 3.4.4. A definite quaternion algebra over $\mathbb{Q}$ is a ring of the form

$$\mathcal{H} = \mathbb{Q} + \mathbb{Q}\alpha + \mathbb{Q}\beta + \mathbb{Q}\alpha\beta$$

where $\alpha^2, \beta^2 \in \mathbb{Q}, \alpha^2 < 0, \beta^2 < 0$ and $\alpha\beta = -\beta\alpha$.

Theorem 3.4.5. Let $\mathcal{R}$ be a characteristic 0 ring with no zero divisors. If $\mathcal{R}$ is a finitely generated $\mathbb{Z}$-module of rank ≤ 4 and further satisfies the following properties

a. $\mathcal{R}$ has an anti-involution $\alpha \mapsto \hat{\alpha}$ with

$$\widehat{\alpha+\beta} = \hat{\alpha}+\hat{\beta}, \quad \hat{\hat{\alpha}} = \alpha, \quad \widehat{\alpha\beta} = \hat{\beta}\hat{\alpha} \text{ for all } \alpha \in \mathcal{R} \quad \text{and} \quad \hat{\alpha} = \alpha \text{ for all } \alpha \in \mathbb{Z}.$$

b. For every $\alpha \in \mathcal{R}$, $\alpha\hat{\alpha} \in \mathbb{Z}_{\geq 0}$ and $\alpha\hat{\alpha} = 0$ if and only if $\alpha = 0$.

Then $\mathcal{R} = \mathbb{Z}$ or $\mathcal{R}$ is an order in an imaginary quadratic number field or $\mathcal{R}$ is an order in a definite quaternion algebra over $\mathbb{Q}$.

Proof. Consider the product $\mathcal{H} = \mathcal{R} \otimes \mathbb{Q}$. Note that an arbitrary element of $\mathcal{H}$ looks like $\sum_j r_j \otimes q_j$ where $r_j \in \mathcal{R}$ and $q_j \in \mathbb{Q}$. So we extend the anti-involution on $\mathcal{R}$ to $\mathcal{H}$ by $r \otimes q \mapsto \hat{r} \otimes q$. Thus with this extended anti-involution, $\mathbb{Q}$ is fixed, i.e $\hat{\alpha} = \alpha$ for all $\alpha \in \mathbb{Q}$ and $\alpha\hat{\alpha} \in \mathbb{Q}_{\geq 0}$. We define a norm and trace (from $\mathcal{H}$ to $\mathbb{Q}$) in the following way

$$\mathrm{N}\alpha = \alpha\hat{\alpha} \text{ and } \mathrm{Tr}\ \alpha = \alpha + \hat{\alpha}.$$

Lemma 3.4.6. The trace and the norm exhibit the following properties

a. $\mathrm{Tr}\,\alpha = 1 + \mathrm{N}\alpha - \mathrm{N}(\alpha - 1)$

b. Tr is $\mathbb{Q}$-linear

c. If $\alpha \in \mathbb{Q}$, then $\mathrm{Tr}\,\alpha = 2\alpha$

d. If $\alpha \in \mathcal{H}$, $\alpha \neq 0$ such that $\mathrm{Tr}\,\alpha = 0$, then $\alpha^2 < 0$ and $\alpha^2 \in \mathbb{Q}$.

Proof. a) we note that

$$\begin{aligned} 1 + \mathrm{N}\alpha - \mathrm{N}(\alpha - 1) &= 1 + \alpha\hat{\alpha} - (\alpha - 1)\widehat{(\alpha - 1)} \\ &= 1 + \alpha\hat{\alpha} - \alpha\hat{\alpha} + \alpha + \hat{\alpha} - 1 \\ &= \mathrm{Tr}\,\alpha \end{aligned}$$

This property implies that for $\alpha \in \mathcal{H}, \mathrm{Tr}\,\alpha \in \mathbb{Q}$

b) Apply the fact that $\hat{\alpha} = \alpha$ for all $\alpha \in \mathbb{Q}$.

c) By the definition of Tr and the fact that the anti-involution fixes $\mathbb{Q}$.

d) Clearly, $0 = (\alpha - \alpha)(\alpha - \hat{\alpha}) = \alpha^2 + \mathrm{N}\alpha$ which implies that $\alpha^2 = -\mathrm{N}\alpha \in \mathbb{Q}$. □

Since $\mathcal{R}$ is a $\mathbb{Z}$-module of rank at most 4, it is enough to show that $\mathcal{H} = \mathbb{Q}$ or an imaginary quadratic number field or a definite quaternion algebra.

If $\mathcal{H} = \mathbb{Q}$, then $\mathcal{R} = \mathbb{Z}$. Otherwise, there exists $\alpha \in \mathcal{H}$ such that $\alpha \notin \mathbb{Q}$. Since $\mathrm{Tr}(\alpha - \frac{1}{2}\mathrm{Tr}\,\alpha) = 0$, we may replace α with $\alpha - \frac{1}{2}\mathrm{Tr}\,\alpha$ and assume that $\mathrm{Tr}\,\alpha = 0$. By Lemma 3.4.6 (d), we have $\alpha^2 < 0$ and $\alpha^2 \in \mathbb{Q}$ so that we can take $\mathcal{H} = \mathbb{Q}(\alpha)$. If $\mathcal{H} \neq \mathbb{Q}(\alpha)$, then we can find $\beta' \in \mathcal{H}$ such that $\beta' \notin \mathbb{Q}(\alpha)$. Let $\beta = \beta' - \frac{\mathrm{Tr}\,\beta'}{2} - \frac{\mathrm{Tr}(\alpha\beta')}{2\alpha^2}\alpha$. Then

$$\begin{aligned}\mathrm{Tr}\,\beta &= \mathrm{Tr}\left(\beta' - \frac{\mathrm{Tr}\,\beta'}{2} - \frac{\mathrm{Tr}(\alpha\beta')}{2\alpha^2}\alpha\right)\\ &= \mathrm{Tr}\,\beta' - \mathrm{Tr}\,\beta' - \frac{\mathrm{Tr}(\alpha\beta')}{2\alpha^2}\mathrm{Tr}\,\alpha\\ &= 0 \qquad \text{since} \quad \mathrm{Tr}\,\alpha = 0.\end{aligned}$$

Replacing β' by β, we may assume that $\mathrm{Tr}\,\beta = 0$. Furthermore, we have

$$\alpha\beta = \alpha\beta' - \frac{\mathrm{Tr}\,\beta'}{2}\alpha - \frac{\mathrm{Tr}(\alpha\beta')}{2}$$

which leads to

$$\mathrm{Tr}(\alpha\beta) = \mathrm{Tr}(\alpha\beta') - \frac{\mathrm{Tr}\,\beta'}{2}\mathrm{Tr}\,\alpha - \mathrm{Tr}(\alpha\beta') = 0.$$

Thus the conditions $\mathrm{Tr}\,\alpha = 0, \mathrm{Tr}\,\beta = 0$ and $\mathrm{Tr}(\alpha\beta) = 0$ imply that

$$\alpha = -\hat{\alpha},\ \ \beta = -\hat{\beta} \text{ and } \alpha\beta = -\hat{\beta}\hat{\alpha}$$

which yield

$$\alpha\beta = -\beta\alpha.$$

Hence $\mathbb{Q}(\alpha, \beta) = \mathbb{Q} + \mathbb{Q}\alpha + \mathbb{Q}\beta + \mathbb{Q}\alpha\beta$ is a definite quaternion algebra. To show that $\mathcal{H} = \mathbb{Q}(\alpha, \beta)$, it suffices to show that 1, α, β, $\alpha\beta$ are linearly independent over $\mathbb{Q}$. Assume we have a relation $r + s\alpha + t\beta + u\alpha\beta = 0$ where $r, s, t, u \in \mathbb{Q}$. Then

$$\mathrm{Tr}(r + s\alpha + t\beta + u\alpha\beta) = 0 \Rightarrow 2r = 0 \Rightarrow r = 0$$

so that $s\alpha + t\beta + u\alpha\beta = 0$. Upon left-multiplication by α and right-multiplication by β, we obtain

$$(\alpha^2 s)\beta + (\beta^2 t)\alpha + u\alpha^2\beta^2 = 0$$

which implies that

$$\alpha^2 s = \beta^2 t = u\alpha^2\beta^2 = 0$$

as $1, \alpha$ and β are linearly independent over $\mathbb{Q}$. Hence $s = t = u = 0$, since $\alpha^2, \beta^2 \neq 0$. This completes the proof. □

Corollary 3.4.7. E/K be an elliptic curve. Then $\mathrm{End}(E)$ is either $\mathbb{Z}$ or an order in an imaginary quadratic number field or an order in a definite quaternion algebra. If char $K = 0$, then $\mathrm{End}(E)$ cannot be an order in a definite quaternion algebra.

Proof. Use Theorem 3.4.5 with $\mathcal{R} = \mathrm{End}(E)$ with the anti-involution being $\alpha \mapsto \hat{\alpha}$ where $\hat{\alpha}$ is the dual isogeny of α.
If char $K = 0$, then $\mathrm{End}(E)$ is commutative. We note that if $\alpha\beta = -\beta\alpha$ with $\alpha, \beta \neq 0$ then $\mathrm{End}(E)$ has zero divisors.

□

Definition 3.4.8. If $\mathrm{End}(E) > \mathbb{Z}$, we say E is an elliptic curve with complex multiplication by $\mathcal{R}$ where $\mathcal{R} \cong \mathrm{End}(E)$ (as rings) is an order given in Theorem 3.4.5

Example 3.4.9. The curve given by

$$y^2 = x^3 + 9x$$

is an elliptic curve over $\mathbb{C}$ with complex multiplication by $\mathbb{Z}[i]$.

Proof. Clearly it is an elliptic curve. We easily check that $\phi : (x, y) \mapsto (-x, iy)$ provides an extra endomorphism. By Corollary 3.4.7, $\mathrm{End}(E)$ is an order in an imaginary quadratic extension of $\mathbb{Q}$. Now $\phi^2(x, y) = (x, -y) = -(x, y)$ so that $\phi^2 = [-1]$. Thus $\mathbb{Z}[i] \hookrightarrow \mathrm{End}(E)$ via $a + bi \mapsto [a] + [b]\phi$. Since by Remark 3.4.3, $\mathbb{Z}[i]$ is maximal in $\mathbb{Q}(i)$, we must have $\mathrm{End}(E) \cong \mathbb{Z}[i]$. □

Chapter 4

Elliptic curves over complex numbers

We use [10] as our reference for this chapter.
We consider elliptic curves defined over $\mathbb{C}$. The main objective in this chapter is to prove that a complex elliptic curve is isomorphic to a torus. A further study is made on the torsion structure.

By a lattice in $\mathbb{C}$, we shall mean a set $L = \mathbb{Z}w_1 + \mathbb{Z}w_2$ where w_1 and w_2 are $\mathbb{R}$-linearly independent complex numbers. Clearly $\mathbb{C}/L$ is a torus. The set

$$\Pi = \{a_1w_1 + a_2w_2 : 0 \leq a_i < 1, i = 1, 2\}$$

is called a *fundamental parallelogram* of L. We set $w_3 = w_1 + w_2$. The fundamental parallelogram is shown in the figure below.

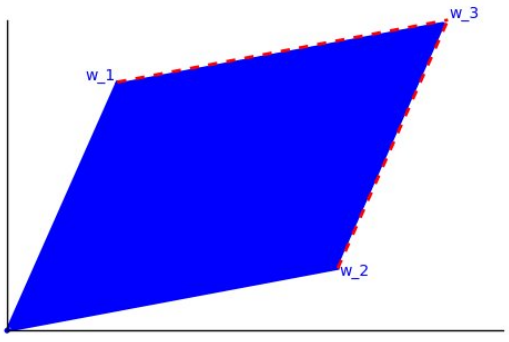


Figure 4.1: The fundamental parallelogram

Note that $z \in \Pi \bmod L$ for every $z \in \mathbb{C}$. A doubly periodic meromorphic (elliptic) function is a function $f : \mathbb{C} \to \mathbb{C} \cup \infty$ such that $f(z+w) = f(z)$ where $w \in L$. If f has no poles, then it is constant. To see this, we use the fact that such a function can only have finitely many poles on a compact subset, on the the closure $\bar{\Pi} = \Pi \cup \partial\Pi$ for instance. The notation $\partial\Pi$ stands for the boundary of Π. Thus f is holomorphic and bounded on $\mathbb{C}$. By Liouvilles's theorem, f is constant.

Theorem 4.0.10. Let f be an elliptic function. We have

a. $\sum_{w\in\Pi} \operatorname{Res}_w(f) = 0$.

b. If $f \neq 0$, then $\sum_{w\in\Pi} \operatorname{ord}_w(f) = 0$ and $\sum_{w\in\Pi} \operatorname{ord}_w(f) w \in L$.

c. If f is non-constant then it is surjective. Let m be the sum of orders of poles of f in Π. Then $f(z) = z_0$ for any $z_0 \in \mathbb{C}$ has m solutions (counting multiplicities).

d. If f has a single pole in Π, then it cannot be simple.

Proof. Cauchy's theorem states that

$$\sum_{w\in\Pi} \operatorname{Res}_w(f) = \frac{1}{2\pi i} \int_{\partial\Pi} f(z)dz$$

The integral splits as follows

$$\int_{\partial\Pi} f(z)dz = \int_0^{w_2} f(z)dz + \int_{w_2}^{w_1+w_2} f(z)dz + \int_{w_1+w_2}^{w_1} f(z)dz + \int_{w_1}^{0} f(z)dz$$

and by periodicity of f and changing sign, we have

$$\int_{w_1+w_2}^{w_1} f(z)dz = -\int_0^{w_2} f(z)dz \text{ and } \int_{w_2}^{w_1+w_2} f(z)dz = -\int_{w_1}^{0} f(z)dz.$$

Consequently (a) holds. If there is a pole on $\partial\Pi$, proper adjustment to the integral can be made, and still yields the same result.

Recall that $\operatorname{Res}_w(\frac{f'}{f}) = \operatorname{ord}_w(f)$. Furthermore, $f'(z+w) = f'(z)$ where $w \in L$. It follows that $\frac{f'}{f}$ is elliptic. By (a), we have $\sum_{w\in\Pi} \operatorname{Res}_w(\frac{f'}{f}) = 0 \Rightarrow \sum_{w\in\Pi} \operatorname{ord}_w(f) = 0$.

From residue calculus, the following identity is verifiable

$$\sum_{w\in\Pi} \operatorname{ord}_w(f) w = \frac{1}{2\pi i} \int_{\partial\Pi} z \frac{f'(z)}{f(z)} dz.$$

We split the integral as done before and for $\int_{w_2+w_1}^{w_1} z\frac{f'(z)}{f(z)}dz$, set $\tilde{z} = z - w_1$. Then the path of integration is the line segment from w_2 to 0, and $d\tilde{z} = dz$. Again by periodicity of $\frac{f'}{f}$, we have

$$\int_{w_2+w_1}^{w_1} z\frac{f'(z)}{f(z)}dz = \int_{w_2}^{0}(z+w)\frac{f'(z)}{f(z)}dz = -\int_0^{w_2} z\frac{f'(z)}{f(z)}dz - w\int_0^{w_2}\frac{f'(z)}{f(z)}dz.$$

The line segment from 0 to w_2 can be parametrized by tw_2 with $0 \leq t \leq 1$, and it is thus clear that $\frac{1}{2\pi i}\int_0^{w_2}\frac{f'(z)}{f(z)}dz$ defines the winding number of the path $z = f(tw_2), 0 \leq t \leq 1$, around 0. Since $f(0) = f(w_2)$, i.e the path is closed, the winding number is an integer and so

$$\int_0^{w_2} z\frac{f'(z)}{f(z)}dz + \int_{w_2+w_1}^{w_1} z\frac{f'(z)}{f(z)}dz \in 2\pi i\mathbb{Z}w_1.$$

By a similar approach, we arrive at

$$\int_{w_1}^{0} z\frac{f'(z)}{f(z)}dz + \int_{w_2}^{w_1+w_2} z\frac{f'(z)}{f(z)}dz \in 2\pi i\mathbb{Z}w_2.$$

Hence $\sum_{w\in\Pi}\mathrm{ord}_w(f)w \in L$, completing the proof of (b).

To establish (c), since f is not constant, it must have at least a pole or zero. Let $z_0 \in \mathbb{C}$, then $f(z) - z_0$ has n zeroes (counting multiplicity) in Π by the second part of (b).

Suppose f has a single pole in Π. Then $\mathrm{Res}_w(f) \neq 0$, and being the only pole implies $\sum_{w\in\Pi}\mathrm{Res}_w(f) \neq 0$, which cannot happen. So either there must be other simple poles or the pole has order at least 2. □

A divisor D is a formal finite sum of points given by

$$D = \sum_{w\in\Pi} n_i[w_i]$$

where $w_i \in \Pi$ and $n_i \in \mathbb{Z}$. The degree of D denoted by $\deg D$ is equal to $\sum n_i$. Note that this is similar to divisors on algebraic curves.

Definition 4.0.11. We define the divisor of a function f to be

$$\mathrm{div}(f) = \sum_{w\in\Pi}\mathrm{ord}_w(f)[w].$$

Lemma 4.0.12. For an integer $k > 2$, we have that

$$\sum_{\substack{w\in L\\ w\neq 0}}\frac{1}{|w|^k}$$

converges.

Proof. See [8]. □

For a lattice L, we define the Weierstrass $\wp$-function to be

$$\wp(z) = \wp(z, L) = \frac{1}{z^2} + \sum_{\substack{w \in L \\ w \neq 0}} \frac{1}{(z-w)^2} - \frac{1}{w^2}.$$

Proposition 4.0.13. The function $\wp(z)$ has the following properties

a. The defining series converges absolutely and uniformly on compact subsets of $\mathbb{C}$ not containing elements of L.

b. $\wp(z)$ is meromorphic, $\wp(-z) = \wp(z)$ and $\wp(z+w) = \wp(z)$ for all $w \in L$.

Proof. Let D be a compact subset of $\mathbb{C}$ such that $D \subset \mathbb{C} - L$. Let $R = \sup\{|z| : z \in D\}$. Consider $|w| \geq 2R$. Let $z \in D$. Then $|z-w| \geq |w| - |z| \geq |w| - R \geq |w| - \frac{|w|}{2} = \frac{|w|}{2}$ and $|2w - z| \leq 2|w| - \frac{|w|}{2} \leq \frac{5}{2}|w|$. Now $\left|\frac{1}{(z-w)^2} - \frac{1}{w^2}\right| = \frac{|z||2w-z|}{|w|^2|z-w|^2} \leq \frac{10R}{|w|^3}$. Note that part of the series with $w \in L$ such that $|w| < 2D$ is convergent since $\{w \in L : |w| < 2D\}$ is finite. By Proposition 4.0.12, the defining series converges absolutely and thus uniformly by the Weierstrass M-test on D. This proves (a). The uniform limit of holomorphic functions is holomorphic, and so we conclude that $\wp(z)$ is holomorphic on $z \notin L$. Furthermore since $(z-w)^2 - \frac{1}{w^2}$ is meromorphic, $\wp(z)$ is meromorphic. From the series expansion, it is clear that $\wp(z)$ has a double pole at each $z \in L$.

The lattice L is an additive subroup of $\mathbb{C}$, so

$$\sum_{\substack{w \in L \\ w \neq 0}} \frac{1}{(-z-w)^2} = \sum_{\substack{w \in L \\ w \neq 0}} \frac{1}{(-z+w)^2} = \sum_{\substack{w \in L \\ w \neq 0}} \frac{1}{(z-w)^2}$$

so that $\wp(-z) = \wp(z)$.

For the other case, we note that $\wp'(z) = -\sum_{w \in L} \frac{1}{(z-w)^3}$ which gives $\wp'(z+w) = \wp'(z)$. Hence there is $e_w \in \mathbb{C}$ such that $e_w = \wp(z+w) - \wp(z)$ for all $z \notin L$. Let $z = -\frac{w}{2}$. Then $e_w = \wp(\frac{w}{2}) - \wp(-\frac{w}{2}) = 0 \Rightarrow \wp(z+w) = \wp(z)$. □

For a lattice L, the Weierstrass σ-function is defined as

$$\sigma(z) = \sigma(z, L) = z \prod_{\substack{w \in L \\ w \neq 0}} \left(1 - \frac{z}{w}\right) e^{z/w + \frac{1}{2}(z/w)^2}.$$

Some of its properties are summarized in the following proposition.

Proposition 4.0.14. The Weierstrass σ-function has the following properties

a. $\sigma(z)$ is analytic.

b. $\sigma(z)$ has simple zeros at $w \in L$ and no other zeros.

c. $\frac{d^2}{dz^2} \log \sigma(z) = -\wp(z)$.

d. For $w \in L$, there exist constants $c = c_w, d = d_w$ such that

$$\sigma(z + w) = e^{cz+d} \text{ for all } z \in \mathbb{C}.$$

Proof. a) Note that $(1 - y)e^{y+\frac{1}{2}y^2} = 1 + b_1 y^3 + b_2 y^4 + \ldots$. So for y near 0, we have

$$|(1 - y)e^{y+\frac{1}{2}y^2} - 1| = C|y|^3$$

for some constant C. The inequality still holds when $y = \frac{z}{w}$ for sufficiently large $|w|$ and z in a compact subset. Since $\sum |\frac{z}{w}|^3$ converges by Lemma 4.0.12, it follows that $\sum \left((1 - \frac{z}{w})e^{\frac{z}{w}+\frac{1}{2}(\frac{z}{w})^2} - 1\right)$ converges. From theory of infinite products, we know that if $\sum_n |b_n|$ converges then $\prod_n (1+b_n)$ converges. Thus $\sigma(z)$ converges uniformly on compact subsets, and so $\sigma(z)$ is analytic for all $z \in \mathbb{C}$.

Part (b) is clear from the definition of $\sigma(z)$.

c) We compute that

$$\frac{d}{dz} \log \sigma(z) = \frac{1}{z} + \sum_{\substack{w \in L \\ w \neq 0}} \left(\frac{1}{z - w} + \frac{1}{w} + \frac{z}{w^2} \right)$$

which implies that

$$\frac{d^2}{dz^2} \log \sigma(z) = -\frac{1}{z^2} + \sum_{\substack{w \in L \\ w \neq 0}} -\frac{1}{(z - w)^2} + \frac{1}{w^2}$$

$$= -\wp(z).$$

d) Let $w \in L$. By chain rule $\frac{d}{dz} \log \sigma(z + w) = \frac{d}{dz} \log \sigma(z)$, so that

$$\frac{d^2}{dz^2} \log \frac{\sigma(z + w)}{\sigma(z)} = 0.$$

Hence $\log \frac{\sigma(z+w)}{\sigma(z)} = cz + d$ and exponentiation yields the desired result. For possible branches of the logarithm that may give rise to complications, refer to [10]. □

Theorem 4.0.15. Let $D = \sum n_i[w_i]$ with $\deg D = 0$ and $\sum n_i w_i \in L$. Then there exists an elliptic function g such that $\operatorname{div}(g) = D$.

Proof. Let $v = \sum n_i w_i$ and $g(z) = \frac{\sigma(z)}{\sigma(z-v)} \prod_i \sigma(z - w_i)^{n_i}$. Let $w \in L$. Then

$$\frac{g(z+w)}{g(z)} = \frac{\sigma(z-v+w)}{\sigma(z-v)}^{-1} \frac{\sigma(z+w)}{\sigma(z)} \prod_i \left(\frac{\sigma(z-w_i+w)}{\sigma(z-w_i)} \right)^{n_i}.$$

But by Proposition 4.0.14 (d), there exist constants a, b depending on w such that

$$\begin{aligned} \frac{g(z+w)}{g(z)} &= e^{az+b} \cdot e^{-az+av-b} \prod_i e^{n_i(a(z-w_i)+b)} \\ &= 1 \quad \text{since} \quad \sum_i n_i = 0. \end{aligned}$$

Therefore the function is elliptic. We also note that $\frac{\sigma(z)}{\sigma(z-v)}$ is analytic at all $z = w_i$ which means that the zeros or poles for g come from $\prod_i \sigma(z - w_i)^{n_i}$. Thus $\operatorname{div}(g) = D$. Indeed g is one such function that we desire. □

4.1 Complex tori as elliptic curves

Definition 4.1.1. Associated to L and for an integer $k \geq 3$, the Eisenstein series is given by

$$G_k = G_k(L) = \sum_{\substack{w \in L \\ w \neq 0}} w^{-k}.$$

Clearly $G_k = 0$ for k odd as $w \in L \Leftrightarrow -w \in L$.

Proposition 4.1.2. The functions $\wp(z)$ and $\wp'(z)$ satisfy the relation

$$\wp'(z)^2 = 4\wp(z)^3 - 60G_4\wp(z) - 140G_6.$$

Proof. We will deduce the Laurent expansion of $\wp(z)$ near 0. Recall that for $|x| < 1$,

$$\frac{1}{1-x^2} = \sum_{n \geq 0} (n+1)x^n.$$

For $|z| < |w|$, we have

$$\frac{1}{(z-w)^2} - \frac{1}{w^2} = \frac{1}{w^2} \left(\frac{1}{(1-\frac{z}{w})^2} - 1 \right) = \sum_{n \geq 1} (n+1) \frac{z^n}{w^{n+2}}.$$

which yields

$$\begin{aligned}\wp(z) &= \frac{1}{z^2} + \sum_{\substack{w\in L\\ w\neq 0}}\sum_{n=1}^{\infty}(n+1)\frac{z^n}{w^{n+2}} \\ &= \frac{1}{z^2} + \sum_{n=1}^{\infty}(n+1)z^n\sum_{\substack{w\in L\\ w\neq 0}}\frac{1}{w^{n+2}} \\ &= \frac{1}{z^2} + \sum_{i=1}^{\infty}(2i+1)z^{2i}\sum_{\substack{w\in L\\ w\neq 0}}\frac{1}{w^{2j+2}} \\ &= \frac{1}{z^2} + \sum_{i=1}^{\infty}(2i+1)G_{2i+2}z^{2i} \\ &= \frac{1}{z^2} + 3G_4z^2 + 5G_6z^4 + \dots\end{aligned}$$

and so

$$\wp'(z) = -\frac{2}{z^3} + 6G_4z + 20G_6z^3 + \dots$$

By expansion, we obtain

$$\wp(z)^3 = \frac{1}{z^6} + \frac{9}{z^2}G_4 + 15G_6 + \dots$$

$$\wp'(z) = \frac{4}{z^6} - \frac{24}{z^2}G_4 - 80G_6 + \dots$$

and note that $g(z)$ defined by

$$g(z) = \wp'(z)^2 - 4\wp(z)^3 + 60G_4\wp(z) + 140G_6$$

has no constant term and no negative powers of z and clearly $g(z) \in \mathbb{C}(\wp(z), \wp(z))$. So $g(z)$ is doubly periodic and is holomorphic at 0. Hence it has no poles. Thus $g(z)$ is constant. Using its series expansion, we note that $g(z) = 0$. This yields the desired result.

□

We shall let $g_3 = 140G_6$ and $g_2 = 60G_4$. Note that the discriminant of the polynomial $4x^3 - g_2x - g_3$ is $16(g_2^3 - 27g_3^2)$.

Proposition 4.1.3. $g_2^3 - 27g_3^2 \neq 0$

Proof. As $\wp'(z)$ is elliptic, we have $\wp'(z+w_i) = \wp'(z)$ for all $z \in \mathbb{C}$ and $i = 1, 2, 3$. Set $z = -\frac{w_i}{2}$. Then $\wp'(-\frac{w_i}{2}) = \wp'(\frac{w_i}{2})$. From the relation $\wp'(-z) = -\wp'(z)$, it follows that $\wp'(\frac{w_i}{2}) = 0$. Hence $\wp(\frac{w_i}{2})$ is a root of the polynomial $4x^3 - g_2x - g_3$. We now show that the roots of the polynomial are distinct.

Let $f_i(z) = \wp(z) - \wp(\frac{w_i}{2})$. Then $f_i(\frac{w_i}{2}) = 0$ and $f_i'(\frac{w_i}{2}) = 0$. Thus $f_i(z)$ has a vanishing order of at least 2 at $\frac{w_i}{2}$. But $f_i(z)$ has only one pole in Π at $z = 0$, and it is a double pole. By Theorem 4.0.10 (c), $\frac{w_i}{2}$ is the only root of $f_i(z)$. So $f_i(\frac{w_j}{2}) \neq 0$ for $i \neq j$ which implies that $4x^3 - g_2x - g_3$ has distinct roots. □

Consequently $E : y^2 = 4x^3 - g_2x - g_3$ is an elliptic curve. We have the following theorem.

Theorem 4.1.4. Let $E/\mathbb{C}$ be the elliptic curve defined by $y^2 = 4x^3 - g_2x - g_3$ and L be a lattice. Then the map $\Phi : \mathbb{C}/L \to E(\mathbb{C})$ given by

$$z \mapsto (\wp(z), \wp'(z))$$
$$0 \mapsto O$$

is a group isomorphism.

Proof. We divide the proof into two parts. The first shows bijectivity and the second shows that Φ is a homomorphism.

Let $(x, y) \in E(\mathbb{C})$. Consider the function $\wp(z) - x$. This function has a double pole, and so it has zeros. Hence, there is $z \in \mathbb{C}$ such that

$$\wp(z) = x \text{ and } \wp'(z)^2 = y^2.$$

Thus $\wp'(z) = \pm y$. If $\wp(z) = y$, then we are done. Now suppose that $\wp'(z) = -y$. Then $\wp'(-z) = y$. We also have $\wp(-z) = \wp(z) = x$ so that $-z \mapsto (x, y)$. Surjectivity is proved. Suppose $(\wp(z_1), \wp'(z_1)) = (\wp(z_2), \wp'(z_2))$. If z_1 is a pole of $\wp(z)$, then $z_1, z_2 \in L$ since $\wp(z)$ only has poles in L and no where else. Then $z_1 \equiv z_2 \bmod L$. On the other hand, if z_1 is not a pole of $\wp(z)$, then $z_1 \notin L$. Since $\wp(z)$ has a double pole at $z = 0$ and no other poles in Π, it follows that $r(z) = \wp(z) - \wp(z_1)$ has a double pole at $z = 0$ and no other poles in Π. By Theorem 4.0.10 (c), $r(z)$ has two zeros.

Suppose $z_1 = \frac{w_i}{2}$ for some $i \in \{1, 2, 3\}$. Since $\wp'(\frac{w_i}{2}) = 0$, z_1 is a double zero of $r(z)$, and thus the only zero. By our earlier assumption, we know that z_2 is a root of $r(z)$. Hence

$z_1 = z_2 \Rightarrow z_1 \equiv z_2 \mod L$.

Now suppose that $z_1 \neq \frac{w_i}{2}$ for some $i \in \{1,2,3\}$. Then $2z_1 \notin L \Rightarrow z_1 + z_1 \not\equiv 0 \mod L$. But $r(z_1) = r(-z_1) = 0$ implies that the two zeros of $r(z)$ are $z_1 \mod L$ and $-z_1 \mod L$. So we must have $z_2 \equiv -z_1 \mod L$. We also have

$$y = \wp'(z_2) = \wp'(-z_1) = -\wp'(z_1) = -y$$

which implies $\wp'(z_1) = 0$. We know that $\wp'(z)$ has only triple pole in Π, and thus it has three zeros. We also know that $\frac{w_i}{2}$ are the three zeros of $\wp'(z)$. This contradicts our assumption that $z_1 \neq \frac{w_i}{2}$ for some $i \in \{1,2,3\}$. Thus $z_1 \equiv z_2 \mod L$, establishing injectivity.

We now prove the homomorphism property of Φ. Let $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$ be distinct points such that the straight line passing through them intersects E at point $P_3 = (x_3, y_3)$ such that $P_3 \neq P_1$ and $P_3 \neq P_2$. We set $P_i = \Phi(z_i)$.

Let $y = \lambda x + \mu$ be the straight line through P_1 and P_2. By computing the addition formula, we note that

$$\begin{aligned} x_3 &= \frac{1}{4}\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 \\ &= \frac{1}{4}\left(\frac{\wp'(z_2) - \wp'(z_1)}{\wp(z_2) - \wp(z_1)}\right)^2 - \wp(z_1) - \wp(z_2). \end{aligned}$$

From the line, we see that $\wp'(z_i) = \lambda\wp(z_i) + \mu$ so that the function $t(z) = \wp'(z) - \lambda\wp(z) - \mu$ has zeros at z_1, z_2 and z_3. However $t(z)$ is elliptic and has a triple pole at $z = 0$ and no poles in Π. Hence $t(z)$ has three zeroes in $\mathbb{C}$. Thus $\operatorname{div}(t) = [z_1] + [z_1] + [z_1] - 3[O]$ which implies that $\sum_{w \in L} \operatorname{ord}_w(t) \cdot w \in L$ by Theorem 4.0.10 (b). We have $z_1 + z_2 + z_3 \in L \Rightarrow z_1 + z_2 = -z_3 \mod L \Rightarrow \wp(z_1 + z_3) = \wp(-z_3) = \wp(z_3) = x_3$. So we have

$$\wp(z_1 + z_2) = \frac{1}{4}\left(\frac{\wp'(z_2) - \wp'(z_1)}{\wp(z_2) - \wp(z_1)}\right)^2 - \wp(z_1) - \wp(z_2). \tag{4.1.1}$$

Fixing z_1 and differentiating the left hand side of Equation 4.1.1, we obtain an expression of $\wp'(z_1 + z_2)$ in terms of $x_i = \wp(z_i), y_i = \wp'(z_i)$ for $i = 1, 2$ and $\wp''(z_2)$. From the Weierstrass equation, we note that

$$2\wp''(z) = 12\wp(z)^2 - g_2 \text{ for } \wp'(z) \neq 0. \tag{4.1.2}$$

For the case $\wp'(z) = 0$, refer to [10]. Setting $z = z_2$ and substituting in the the expression for $\wp''(z_1 + z_2)$ and performing some algebraic manipulation, we get $-y_3 = \wp'(z_1 + z_2)$. Thus

$$\Phi(z_1 + z_2) = \Phi(z_1) + \Phi(z_2). \tag{4.1.3}$$

We now look at the cases where $\wp(z_1 + z_2)$ in Equation 4.1.1 is not defined, i.e $\wp(z_i) = \infty$ or $z_1 = -z_2$.

When $\wp(z_i) = \infty$, then z_i is a pole and poles of $\wp(z)$ only occur at points in L. So $z_i = 0$. Hence $(\wp(0), \wp(0)) = O$ which shows that Equation 4.1.3 is true. For $z_1 = -z_2$, we have $z_1 + z_2 = 0 \mod L$ so that $\Phi(z_1 + z_2) = O$. We also note that

$$(\wp(z_2), \wp'(z_2)) = (\wp(z_1), \wp'(-z_1)) = (\wp(z_1), -\wp'(z_1)) = -(\wp(z_1), \wp'(z_1))$$

which implies $(\wp(z_1), \wp'(z_1)) + (\wp(z_2), \wp'(z_2)) = O$. Thus Equation 4.1.1 is true. For the case when $z_1 = z_2$, we note that $\frac{\wp'(z_2)-\wp'(z_1)}{\wp(z_2)-\wp(z_1)} \to \frac{\wp''(z_2)}{\wp'(z_2)}$ as $z_1 \to z_2$ by L'Hopital's rule and using Equations 4.1.1 and 4.1.2, we have

$$\wp(2z_1) = \frac{1}{4}\left(\frac{6\wp(z_1)^2 - \frac{1}{2}g_2}{\wp'(z_1)}\right)^2 - 2\wp(z_1).$$

Using appropriate group law formulas, it can be shown that if $x_1 = x_3$, then

$$x_3 = \frac{1}{4}\left(\frac{12x_1 - g_2}{2y_1}\right)^2 - 2x_1.$$

Clearly $x_3 = \wp(2z_1)$. Differentiating with respect to z_1 yields the right expression for the y-coordinate. □

4.2 Uniformization theorem

We now want to show that every elliptic curve comes from a lattice.

Consider $L = \mathbb{Z}w_1 + \mathbb{Z}w_2$. The $\mathbb{R}$-linear independence of w_1 and w_2 implies that $\tau = \frac{w_1}{w_2} \in \mathbb{C} \setminus \mathbb{R}$. By rearrangement if necessary, we may assume that $\mathrm{Im}(\tau) > 0$. Thus we have another lattice $L_\tau = \mathbb{Z}\tau + \mathbb{Z}$. Since $w_2 L_\tau = L$, the two lattices L_τ and L are homothetic. For an integer $k \geq 3$, define

$$G_k(\tau) = G_k(L_\tau) = \sum_{(r,s)\neq(0,0)} \frac{1}{(r\tau + s)^k}.$$

Then we have $G_k(\tau) = w_2^k G_k(L)$ where $G_k(L)$ is the Eisenstein series for the lattice $L = \mathbb{Z}w_1 + \mathbb{Z}w_2$.

Let $g_2(\tau) = g_2(L_\tau) = 60G_4(\tau)$ and $g_3(\tau) = g_3(L_\tau) = 140G_6(\tau)$. Let $\Delta = g_2^3 - 27g_3^2$ and define

$$j(\tau) = 1728\frac{g_2^3}{\Delta}. \tag{4.2.1}$$

In general, for an arbitrary lattice L, we define $j(L)$ to be

$$j(L) = 1728\frac{g_2(L)^3}{g_2(L)^3 - 27g_3(L)^2}.$$

It can be shown that $j(L)$ converges and we will not concern ourselves of the details of the proof, and for such details we refer you to [10]. So it follows that for any $\lambda \in \mathbb{C}^\times$,

$$g_2(\lambda L) = \lambda^{-4} g_2(L) \text{ and } g_3(\lambda L) = \lambda^{-6} g_3(L).$$

Hence $j(\lambda L) = j(L)$. In particular $j(\mathbb{Z}w_1 + \mathbb{Z}w_2) = j(\tau)$ where $\tau = \frac{w_1}{w_2}$.

Let $\mathbb{H}$ denote the upper half plane. Also note the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}$ given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau = \frac{a\tau + b}{c\tau + d}$$

for all $\tau \in \mathbb{H}$.

Proposition 4.2.1. For any $\tau \in \mathbb{H}$ and $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, we have

$$j(\tau) = j\left(\frac{a\tau + b}{c\tau + d}\right)$$

Proof. By definition, we have

$$\begin{aligned} G_k\left(\frac{a\tau + b}{c\tau + b}\right) &= \sum_{(r,s)\neq(0,0)} \frac{1}{\left(r\frac{a\tau+b}{c\tau+d} + s\right)^k} \\ &= (c\tau + d)^k \sum_{(r,s)\neq(0,0)} \frac{1}{((ra + sc)\tau + rb + sd)^k} \end{aligned}$$

Let $(r', s') = (ra + sc, rb + sd) = (r, s)\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Then $(r, s) = (r', s')\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1}$. Thus we have a 1-1 correspondence between pairs of integers (r, s) and (r', s'). Hence

$$\begin{aligned} G_k\left(\frac{a\tau + b}{c\tau + b}\right) &= (c\tau + d)^k \sum_{(r',s')\neq(0,0)} \frac{1}{(r'\tau + s')^k} \\ &= (c\tau + d)^k G_k(\tau). \end{aligned}$$

So we note that

$$\begin{aligned} g_2\left(\frac{a\tau+b}{c\tau+b}\right) &= 60G_4\left(\frac{a\tau+b}{c\tau+b}\right) \\ &= (c\tau+d)^4 60G_4(\tau) \\ &= (c\tau+d)^4 g_2(\tau). \end{aligned}$$

Similarly, we have $g_3\left(\frac{a\tau+b}{c\tau+b}\right) = (c\tau+d)^6 g_3(\tau)$. Substituting these expressions in Equation 4.2.1 yields the result. □

Let $\mathbb{H}^f = \{z \in \mathbb{H} : -\frac{1}{2} \leq \mathrm{Re}(z) < \frac{1}{2}, z \neq e^{i\theta} \text{ for } \frac{\pi}{3} < \theta < \frac{\pi}{2}, |z| \geq 1\}$. $\mathbb{H}^f$ is called the fundamental domain of $\mathbb{H}$ under the action of $\mathrm{SL}_2(\mathbb{Z})$.

Proposition 4.2.2. For every $\tau \in \mathbb{H}$, there is $M \in \mathrm{SL}_2(\mathbb{Z})$ such that $M\tau \in \mathbb{H}^f$ and $M\tau$ is uniquely determined by τ.

Proof. See [10]. □

Corollary 4.2.3. For any lattice L, there exists a basis $\{w_1, w_2\}$ such that $\frac{w_1}{w_2} \in \mathbb{H}^f$.

Proof. Let $\{y_1, y_2\}$ be a basis of L. Performing a rearrangement if necessary, we may assume that $t = \frac{y_1}{y_2} \in \mathbb{H}$. By Proposition 4.2.2, let $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ be such that $\frac{at+b}{ct+d} \in \mathbb{H}^f$. Set $w_1 = ay_1 + by_2$ and $w_2 = cy_1 + dy_2$. Clearly, $\mathbb{Z}y_1 + \mathbb{Z}y_2 = \mathbb{Z}w_1 + \mathbb{Z}w_2$ since $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is invertible. Furthermore,

$$\frac{w_1}{w_2} = \frac{ay_1 + by_2}{cy_1 + dy_2} = \frac{a(y_1/y_2) + b}{c(y_1/y_2) + d} = \frac{at+b}{ct+d} \in \mathbb{H}^f.$$

□

Proposition 4.2.4. For every complex number z, there is exactly one $\tau \in \mathbb{H}^f$ such that $j(\tau) = z$.

Proof. See [8]. □

Corollary 4.2.5. Let τ_1 and τ_2 be elements in $\mathbb{H}$. Then $j(\tau_1) = j(\tau_2)$ if and only if there exists $M \in \mathrm{SL}_2(\mathbb{Z})$ such that $M\tau_1 = \tau_2$.

Proof. If there exists $M \in \mathrm{SL}_2(\mathbb{Z})$ such that $M\tau_1 = \tau_2$, then Proposition 4.2.1 tells us that $j(\tau) = j(M\tau) = j(\tau)$.
Conversely, suppose that $j(\tau_1) = j(\tau_2)$. By Proposition 4.2.2, there exist $M', M'' \in \mathrm{SL}_2(\mathbb{Z})$ such that

$$M'\tau_1 = \tau_1' \in \mathbb{H}^f \text{ and } M''\tau_2 = \tau_2' \in \mathbb{H}^f.$$

So we observe that $j(\tau_1) = j(M'\tau_1) = j(\tau_1')$ and $j(\tau_2) = j(M''\tau_2) = j(\tau_1')$ which implies that $j(\tau_1') = j(\tau_2')$. By Proposition 4.2.4, it follows that $\tau_1' = \tau_2'$.
It is not difficult to see that $M''\tau_2 = \tau_2'$ for $M'' \in \mathrm{SL}_2(\mathbb{Z})$ implies that $N''\tau_2' = \tau_2$ for some $N'' \in \mathrm{SL}_2(\mathbb{Z})$. Thus we can find $M \in \mathrm{SL}_2(\mathbb{Z})$ such that $M\tau_1 = \tau_2$. □

Corollary 4.2.6. Let L', L'' be arbitrary lattices in $\mathbb{C}$. Then $j(L') = j(L'')$ if and only if $L' = cL'$ for some constant $c \in \mathbb{C}^\times$.

Proof. If $L' = cL', c \in \mathbb{C}^\times$, then we saw earlier that $j(cL') = j(L')$ so that this direction is verified.
Conversely, if $j(L') = j(L')$. By Corollary 4.2.3, $L' = r_1 L_{\tau_1}$ and $L'' = r_2 L_{\tau_2}$ for some $\tau_i \in \mathbb{H}^f$ and $r_i \in \mathbb{C}^\times$, $i = 1, 2$. So we have

$$j(L_{\tau_1}) = j(\tau_1) = j(L_{\tau_2}) = j(\tau_2)$$

and by Proposition 4.2.4, we have $\tau_1 = \tau_2$. Setting $c = \frac{r_1}{r_2}$, we have $L' = cL''$. □

Theorem 4.2.7. Let $E/\mathbb{C}$ be an elliptic curve defined by the equation $y^2 = 4x^3 - Ax - B$. Then there exists a lattice L such that $g_2(L) = A$ and $g_3(L) = B$. Furthermore, we have a group isomorphism $\mathbb{C}/L \cong E(\mathbb{C})$.

Proof. Let $z = 1728\frac{A^3}{A^3 - 27B^2}$. Proposition 4.2.4 implies that there is a lattice $T = \mathbb{Z}\tau + \mathbb{Z}$ where $\tau \in \mathbb{H}^f$ such that $j(T) = j(\tau) = z$, i.e

$$1728\frac{g_2(T)^3}{g_2(T)^3 - 27g_3(T)^2} = 1728\frac{A^3}{A^3 - 27B^2}. \tag{4.2.2}$$

We investigate the following situations.
Case I: Suppose $g_2(T) \neq 0$. Then $A \neq 0$ since $g_2(T)^3 - 27g_3(T)^2 \neq 0$ by Proposition 4.1.3 and $A^3 - 27B^2 \neq 0$ as E is an elliptic curve. Choose $c \in \mathbb{C}^\times$ with the property that $g_2(cT) = c^{-4}g_2(T) = A$. Then by some algebraic manipulation of Equation 4.2.2,

we have $g_3(cT)^2 = B^2 \Rightarrow g_3(cT) = \pm B$. If $g_3(cT) = B$, then $L = cT$ is a desired lattice. Otherwise, we observe that

$$g_3(icT) = i^{-6}g_3(cT) = -g_3(cT) = B \text{ and } g_2(icT) = i^{-4}g_2(cT) = A$$

so that $L = icT$ is a desired lattice.

Case II: Assume $g_2(T) = 0$. Then $A = 0$, $B \neq 0$ and $g_3(T) \neq 0$. So choose $d \in \mathbb{C}^\times$ such that $g_3(dT) = d^{-6}g_3(T) = B$. Then $g_2(dT) = d^{-4}g_2(T) = 0$. Thus $L = dT$ is a desired lattice.

By Theorem 4.1.4, $\mathbb{C}/L \cong E(\mathbb{C})$. □

The structure of $E[m]$ is now easy to describe. Since there exists a lattice $L = \mathbb{Z}w_1 + \mathbb{Z}w_2$ such that $E(\mathbb{C}) \cong \mathbb{C}/L$ and that we can identify $\mathbb{C}/L$ with the fundamental parallelogram, we have that $z \in E[m]$ if and only if $z = \frac{j}{m}w_1 + \frac{k}{m}w_2$ where $0 \leq j, k < m$ and $j, k \in \mathbb{Z}$. Thus

$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

which also confirms the result in chapter three on the structure of m-torsion subgroup when char $K = 0$. We demonstrate this with an example for $m = 2, 3$.

Example 4.2.8 (The case of $m = 2$)**.** Let $E/\mathbb{C}$ be given by the equation $y^2 = f(x)$ where

$$f(x) = x^3 + ax^2 + bx + c.$$

For $m = 2$, recall that P has order two if and only if $2P = \mathcal{O}$ and $P \neq \mathcal{O}$. But $2P = \mathcal{O}$ implies $P = -P$ so that $x(P) = x(-P)$. This means that the y-coordinate of P must be zero. Conversely, if $P = (x, 0)$, then the tangent at P is vertical so that $2P = \mathcal{O}$. Hence points of order two are exactly those points whose y coordinate is equal to zero. We have to solve the equation $f(x) = 0$, for the x coordinates. By the fundamental theorem of algebra, f has three complex roots. We have three points $P \neq \mathcal{O}$ with order dividing 2. Together with $\mathcal{O}$, the three points of order two form an abelian subgroup of $E(\mathbb{C})$. Thus

$$E[2] \cong Z/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

since there are no points of order 4.

Example 4.2.9 (The case of $m = 3$)**.** We now look at the case when $m = 3$ using the curve defined in Example 4.2.8. If P has order three, then $3P = \mathcal{O}$ which is the same as saying $2P = -P$. So we have $x(2P) = x(P)$. We claim that if $x(2P) = x(P)$ and $P \neq \mathcal{O}$, then $3P = \mathcal{O}$. That is because $x(2P) = x(P)$ implies that $x(2P) = x(-P)$ so that $2P = \pm P$ which implies $3P = \mathcal{O}$ since $P \neq \mathcal{O}$. Hence points of order three in $E(\mathbb{C})$ are exactly those points that satisfy the equality $x(2P) = x(P)$. Let $P = (x, y)$. Using appropriate group law formulas, we have

$$x^4 - 2bx^2 - 4ac + b^2 - 8cx - 4x(ax^2 + x^3 + bx + c) = 0$$

which results in

$$3x^4 + 4ax^3 + 6bx^2 + 12cx + 4ac - b^2 = 0.$$

So points of order three are the roots of the equation $3x^4+4ax^3+6bx^2+12cx+4ac-b^2 = 0$ Furthermore, we also observe that

$$3x^4 + 4ax^3 + 6bx^2 + 12cx + 4ac - b^2 = 2f(x)f''(x) - f'(x)^2.$$

Denote this polynomial by $\beta(x)$. Then $\beta'(x) = 12f(x)$. We claim that each complex zero of $\beta(x)$ has multiplicity 1. To justify this claim, it is enough to show that $\beta(x)$ and $\beta'(x)$ have no common zero.

Assume that $\beta(x)$ and $\beta'(x)$ have a common zero α, say. It follows that α is a root of $12f(x)$ and $2f(x)f''(x) - f'(x)^2$, i.e $f(\alpha) = 0$ and $2f(\alpha)f''(\alpha) - f'(\alpha)^2 = 0$. Clearly we have $f(\alpha) = 0$ and $f'(\alpha) = 0$ so that α is a common zero of $f(x)$ and $f'(x)$. This implies that E is singular. So we have a contradiction. Hence $\beta(x)$ and $\beta'(x)$ have no common root implying that the polynomial $\beta(x)$ has distinct roots. Since its degree is 4, we have four distinct roots. However note that each root gives two values of y so that we have exactly eight points of order three. Consequently, there are nine points of order dividing three (we have included the identity). Hence $E[3] \cong Z/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

Chapter 5

Elliptic curves over local fields

The references used in this chapter are [8] and [7].

5.1 Formal Groups

Definition 5.1.1. A (*one-parameter commutative*) formal group $\mathcal{F}$ over a ring R is a power series $F(X,Y) \in R[[X,Y]]$ satisfying the following properties:

1. $F(X,Y) = X + Y +$ (terms of higher degree ≥ 2).
2. $F(X,Y) = F(Y,X)$ (Commutativity).
3. $F(X,F(Y,Z)) = F(F(X,Y),Z)$ (Associativity).
4. $F(X,0) = X$ and $F(0,Y) = Y$.
5. There exits a unique $i(T) \in R[[T]]$ such that $F(i(T),T) = 0$ (existence of inverse).

The power series $F(X,Y)$ is called the formal group law of $\mathcal{F}$.

It is easy to see that $F(X,Y) = X + Y$ defines is a formal group with $i(T) = -T$.

Definition 5.1.2. Let $(F,\mathcal{F})$ and $(G,\mathcal{G})$ be formal groups over a ring R. A homomorphism from $\mathcal{F}$ to $\mathcal{G}$ (defined over R) is a power series $f \in R[[T]]$ such that $f(F(X,Y)) = G(f(X),f(Y))$. In addition to the above, if there exists a homomorphism $g : \mathcal{G} \to \mathcal{F}$ with $g(f(T)) = f(g(T)) = T$, then $\mathcal{F}$ and $\mathcal{G}$ are said to be isomorphic over R

Proposition 5.1.3. Let $(F, \mathcal{F})$ be a formal group and $m \in \mathbb{Z}$. Then $[m] : \mathcal{F} \to \mathcal{F}$ defined by

$$[0](T) = 0, \quad [m+1](T) = F([m](T), T), \quad [m-1](T) = F([m](T), i(T))$$

is a homomorphism

Proof. We look at the case $m \geq 0$. Clearly $[0](F(X,Y)) = F([0](X), [0](Y))$. By induction assume the result holds for an integer $k \geq 1$, i.e $[k](F(X,Y)) = F([k](X), [k](Y))$. We need to show that it is true for $k+1$. We proceed as follows:

$$\begin{aligned}
[k+1](F(X,Y)) &= F([k](F(X,Y), F(X,Y)) \text{ by definition} \\
&= F(F([k](X), [k](Y)), F(X,Y)) \text{ by induction hypothesis} \\
&= F([k](X), F([k](Y), F(X,Y))) \text{ by associativity} \\
&= F([k](X), F(F(X,Y), [k](Y))) \text{ by commutativity} \\
&= F([k](X), F(X, F(Y, [k](Y)))) \text{ by associativity} \\
&= F([k](X), F(X, F([k](Y), Y))) \text{ by commutativity} \\
&= F(F([k](X), X), F([k](Y), Y)) \text{ by associativity} \\
&= F([k+1](X), [k+1](Y))
\end{aligned}$$

Before proving for $m \leq -1$, we claim that $iF(X,Y) = F(i(X), i(Y))$. By definition, we have

$$F(F(X,Y), i(F(X,Y))) = 0 \tag{5.1.1}$$

and so using associativity and commutativity, we observe that

$$\begin{aligned}
F(F(X,Y), F(i(X), i(Y))) &= F(X, F(F(i(X), i(Y)), Y)) \\
&= F(F(X, F(i(X), i(Y))), Y).
\end{aligned}$$

But the inner term $F(X, F(i(X), i(Y))) = F(F(X, i(X)), i(Y)) = F(0, i(Y)) = i(Y)$ so that $F(F(X, F(i(X), i(Y))), Y) = F(i(Y), Y) = 0$. By uniqueness of $i(F(X,Y)$ in Equation 5.1.1, we conclude that $F(i(X), i(Y)) = iF(X,Y)$. Let $m = -1$. Then $[-1](F(X,Y)) = F([0](F(X,Y), i(F(X,Y)))) = iF(X,Y)$ which by the above claim

is $F(i(X), i(Y))$. But

$$\begin{aligned} F(i(X), i(Y)) &= F(0, F(i(X), i(Y))) = F(0, F(i(X), F(0, i(Y)))) \\ &= F(F(0, i(X)), F(0, i(Y))) = F([-1](X), [-1](Y)). \end{aligned}$$

Assume it holds for an integer $k < 0$, i.e $[k](F(X, Y) = F([k](X), [k](Y))$. We note that

$$\begin{aligned} [k-1](F(X,Y)) &= F([k](F(X,Y)), i(F(X,Y))) \\ &= F(F([k](X), [k](Y)), F(i(X), i(Y))) \\ &= F(F([k](Y), [k](X)), F(i(X), i(Y))) \\ &= F([k](Y), F([k](X), F(i(X), i(Y)))). \quad \text{But we have} \\ F([k](X), F(i(X), i(Y))) &= F(F([k](X), i(X)), i(Y)) = F([k-1](X), i(Y)) \\ \text{so that} \quad [k-1](F(X,Y)) &= F([k](Y), F([k-1](X), i(Y))) \\ &= F([k](Y), F(i(Y), [k-1](X))) \\ &= F(F([k](Y), i(Y)), [k-1](X)) \\ &= F([k-1](Y), [k-1](X)). \end{aligned}$$

□

Proposition 5.1.4. If $f(T) = a_1T + a_2T^2 + a_3T^3 + a_4T^4 + \ldots \in R[[T]]$ with $a_1 \in R^\times$, then there exists a unique power series $g(T)$ satisfying $f(g(T)) = g(f(T)) = T$.

Proof. Note that constructing a sequence $g_n(T)$ such that $f(g_n(T)) \equiv T \pmod{T^{n+1}}$ and $g_{n+1}(T) \equiv g_n(T) \pmod{T^{n+1}}$, and setting

$$g(T) = \lim_{n\to\infty} g_n(T)$$

proves the existence part. Set $g_1(T) = a_1^{-1}T$ and clearly $f(g_1(T)) \equiv T \pmod{T^2}$. Having defined g_{n-1}, we by induction define

$$g_n(T) = g_{n-1}(T) + \lambda T^n$$

for some $\lambda \in R$ to be determined. So we have

$$\begin{aligned} f(g_n(T)) &= f(g_{n-1}(T) + \lambda T^n) \\ &= a_1(g_{n-1}(T) + \lambda T^n) + a_2(g_{n-1}(T) + \lambda T^n)^2 + a_3(g_{n-1}(T) + \lambda T^n)^3 + \dots \\ &\equiv a_1\lambda T^n + a_1 g_{n-1}(T) + a_2 g_{n-1}(T)^2 + a_3 g_{n-1}(T)^3 + \dots \pmod{T^{n+1}} \\ &\equiv f(g_{n-1}(T)) + a_1\lambda T^n \pmod{T^{n+1}} \\ &\equiv T + cT^n + a_1\lambda T^n \pmod{T^{n+1}} \quad \text{for some} \quad c \in R. \end{aligned}$$

From the relation $f(g_n(T)) \equiv T \pmod{T^{n+1}}$, we obtain $\lambda = -a_1^{-1}c$. By this construction, we have that $g(T) \in R[[T]]$ and satisfies $f(g(T)) = T$. On the other hand, we have $g(T) = a_1^{-1}T +$(terms of higher order) and $a_1^{-1} \in R^\times$. By the above argument, there exists $g'(T) \in R[[T]]$ such that $g(g'(T)) = T$. So $g(f(T)) = g(f(g(g'(T)))) = g(f \circ g(g'(T))) = g(g'(T)) = T$. Finally to prove uniqueness of $g(T)$. Assume that $h(T)$ is another power series satisfying $f(h(T)) = T$. Then $g(T) = g(f \circ h(T)) = (g \circ f)(h(T)) = h(T)$. □

Proposition 5.1.5. Let $\mathcal{F}$ be a formal group over R and $m \in \mathbb{Z}$. Then

a. $[m](T) = mT +$ higher order terms.

b. If $m \in R^\times$, then $[m] : \mathcal{F} \to \mathcal{F}$ is an isomorphism.

Proof. For $m \geq 0$, using the recursive definition of $[m](T)$ given in Proposition 5.1.3 and induction on m yields (a). Now suppose that $m < 0$. By definition, $[-1](T) = F([0](T), i(T)) = F(0, i(T)) = i(T)$. But $F(T, i(T)) = 0 \Rightarrow 0 = T + i(T) + \dots \Rightarrow i(T) = -T + \dots$. Applying a downward induction on m completes the general case $m < 0$.
(b) Follows from Proposition 5.1.4. □

Definition 5.1.6. Let R be a complete local ring with maximal ideal $\mathcal{M}$ and $\mathcal{F}$ a formal group over R. The group associated to $\mathcal{F}/R$, denoted by $\mathcal{F}(\mathcal{M})$, is the set $\mathcal{M}$ endowed with the operations

$$x \oplus y = F(x, y) \text{ for all } x, y \in \mathcal{M} \text{ (addition).}$$

$$\ominus x = i(x) \text{ for all } x \in \mathcal{M} \text{ (inversion).}$$

Note that $\mathcal{F}(\mathcal{M})$ is a group under the stated operations.

Proposition 5.1.7. Let $\mathcal{F}$ be a formal group over a complete local ring R with the maximal ideal $\mathcal{M}$ and $p = \operatorname{char} R/\mathcal{M} > 0$. Then $\mathcal{F}(\mathcal{M})$ is a p-group.

Proof. Let $x \in \mathcal{F}(\mathcal{M})$ be an element of order m. Then $[m](x) = 0$. Write $m = rp^s$ with $(p, r) = 1$. Then we have $[r]([p^s](x)) = 0$. So we can assume that $(m, p) = 1$. Then $[m](x) = 0$ and $m \in R^\times$. By Proposition 5.1.5, $[m] : \mathcal{F}(\mathcal{M}) \to \mathcal{F}(\mathcal{M})$ is an isomorphism, and thus $x = 0$. □

We would like to look at the formal group associated to an elliptic curve. We first discuss the following.

Proposition 5.1.8. (Hensel's Lemma) Let R be a ring that is complete with respect to some ideal $I \subset R$. Suppose $F(T) \in R[T], a \in R, n \in \mathbb{Z}_{\geq 1}$ are such that $F(a) \in I^n$ and $F'(a) \in R^\times$. If $\alpha \equiv F'(a) \pmod{I}$, then

$$w_0 = a, \qquad w_{m+1} = w_m - \frac{F(w_m)}{\alpha}$$

converges to $b \in R$ such that b is a zero of $F(T)$ and $b \equiv a \pmod{I^n}$. If R is an integral domain, then b is unique.

Proof. We replace $F(w)$ by $\frac{F(w+a)}{\alpha}$ so that the above conditions and recurrence become: $F(0) \in I^n,\ F'(0) \equiv 1 \pmod{I}\ , w_0 = 0, w_{m+1} = w_m - F(w_m)$.
We first prove the convergence part. Note that $w_1 = w_0 - F(0) \in I^n \Rightarrow w_2 \in I^n$. Continuing in this manner, we see that if $w_m \in I^n$, then $w_{m+1} \in I^n$ for all $m \geq 0$. By induction, it follows that $w_m \in I^n$ for all $m \geq 0$.
We claim that $w_{m+1} - w_m \in I^{m+n}$ for all $m \geq 0$. Clearly $w_1 - w_0 = -F(0) \in I^n$. By induction, assume it is true for all integers strictly less than m. Note that $F(T) = F(0) + F'(0)T + O(T^2)$, and so we can write

$$F(s) - F(t) = (s - t)(F'(0) + sG(s, t) + tH(s, t)) \text{ for some } G, H \in R[s, t]. \tag{5.1.2}$$

By the recurrence relation, we have

$$w_{m+1} - w_m = w_m - F(w_m) - (w_{m-1} - F(w_{m-1})) = w_m - w_{m-1} - (F(w_m) - F(w_{m-1}))$$

and so using Equation 5.1.2,

$$F(w_m) - F(w_{m-1}) = (w_m - w_{m-1})(F'(0) + w_m G(w_m, w_{m-1}) + w_{m-1}H(w_m, w_{m-1}))$$

so that

$$w_{m+1} - w_m = (w_m - w_{m-1})(1 - F'(0) - w_m G(w_m, w_{m-1}) - w_{m-1}H(w_m, w_{m-1})).$$

Since $1 - F'(0) \in I, w_{m-1}, w_m \in I^n \subseteq I$, it follows that

$$(1 - F'(0) - w_m G(w_m, w_{m-1}) - w_{m-1}H(w_m, w_{m-1})) \in I$$

and by induction hypothesis, $w_m - w_{m-1} \in I^{m-1+n}$, we have $w_{m+1} - w_m \in I^{m-1+n}I = I^{m+n}$. The completeness of R implies convergence of the sequence to an element $b \in I^n$ such that $b = b - F(b)$, i.e $F(b) = 0$.

For the uniqueness part where we assume that R is an integral domain, say $c \in I^n$ is such that $F(c) = 0$. Making use of Equation 5.1.2, observe that $F(b) - F(c) = (b - c)(F'(0) + bG(b, c) + cH(b, c)) = 0$. If $b \neq c$, then $F'(0) = -bG(b, c) - cH(b, c) \in I$ as $b, c \in I$. But this is a contradiction since $F'(0) \notin I$. So we must have $b = c$. □

Definition 5.1.9. Let $\mathcal{F}$ be a formal group over a ring R with the formal group law F. An invariant differential on $\mathcal{F}$ is a differential form $\omega(T) = P(T)dT$ that satisfies $\omega(F(T, S)) = \omega(T)$.

From the definition above, we have

$$\omega(F(T, S)) = \omega(T) \Rightarrow P(F(T, S))d(F(T, S)) = P(T)dT$$

which implies that $P(F(T, S))\frac{\partial}{\partial T}(F(T, S)) = P(T)$. We use $F_1(U, V)$ to mean the partial derivative of F with respect to the first variable. So $w(T) = P(T)dT$ is invariant if $P(F(T, S))F_1(T, S) = P(T)$. If $P(0) = 1$, ω is said to be normalized.

Proposition 5.1.10. For a formal group $\mathcal{F}/R$ with formal group law F, there exists a unique invariant differential given by $F_1(0, T)^{-1}dT$ such that if ω is an invariant differential on $\mathcal{F}$, then $\omega = \lambda F_1(0, T)dT$ for some $\lambda \in R$.

Proof. Let ω be an invariant differential. Now $\omega = P(T)dT$ is such that

$$P(F(T,S))F_1(T,S) = P(T) \Rightarrow P(F(0,S))F_1(0,S) = P(0),$$

i.e $P(S)F_1(0,S) = P(0)$. But

$$F(T,S) = S + T + \text{ higher order terms } \Rightarrow F_1(0,S) = 1 + \text{ higher order terms}$$

so that $F_1(0,T)^{-1} \in R[[T]]$. Thus $P(T) = P(0)F_1(0,T)^{-1}$. Since we know the coefficients of $F_1(0,T)^{-1}$, we just need to know $P(0)$ to completely specify $P(T)$. So if $P(0) = 1$, we have $P(T) = F_1(0,T)^{-1}$ and the differential $F_1(0,T)^{-1}dT$ is unique and normalized differential. As shown above, ω is of the form $\lambda F_1(0,T)^{-1}$. It remains to show that $F_1(0,T)^{-1}dT$ is invariant, i.e

$$F_1(0,F(T,S))^{-1}F_1(T,S) = F_1(0,T)^{-1}.$$

Recall the associativity law $F(X,F(T,S)) = F(F(X,T),S)$. Differentiating with respect to X we have

$$F_1(X,F(T,S)) = \frac{\partial}{\partial R}(F(R,S))F_1(X,T) \text{ where } R = F(X,T),$$

which, in our notation implies that

$$F_1(X,F(T,S)) = F_1(F(F(X,T),S))F_1(X,T).$$

Set $X = 0$, we get

$$F_1(0,F(T,S)) = F_1(F(T,S))F_1(0,T)$$

which yields the desired result. □

Proposition 5.1.11. Let $f : \mathcal{F}/R \to \mathcal{G}/R$ be a homomorphism between formal groups. Let $\omega_{\mathcal{G}}$ and ω_F be normalised invariant differentials on $\mathcal{F}/R$ and $\mathcal{G}/R$, respectively. Then

$$\omega_G \circ f = f'(0)\omega_F.$$

Proof. Denote by $F, G \in R[[X,Y]]$ the formal group laws of $\mathcal{F}$ and $\mathcal{G}$, respectively. Then

$$(\omega_G \circ f)(F(T,S)) = \omega_G(G(f(T),f(S))) = \omega_G(f(T)) = (\omega_G \circ f)(T)$$

Thus $\omega_G \circ f$ is an invariant differential on $\mathcal{F}$. So by Proposition 5.1.10, $\omega_G \circ f = \lambda\omega_F$ for some $\lambda \in R$. To find λ, note that

$$\omega_G(f(T)) = G_1(0, f(T))^{-1} df(T) = G_1(0, f(T))^{-1} f'(T) dT$$

and

$$\lambda\omega_F = \lambda F_1(0, T)^{-1} dT$$

so that

$$f'(T) = \lambda F_1(0, T)^{-1} G_1(0, f(T)) = \lambda(1 + \text{ higher order terms})$$

from which we get $\lambda = f'(0)$. □

Proposition 5.1.12. Given a formal group $\mathcal{F}/R$ and a prime $p \in \mathbb{Z}$. There exist $g(T), h(T) \in R[[T]]$ such that $h(0) = g(0) = 0$ and $[p](T) = ph(T) + g(T^p)$.

Proof. Recall that $[p](T) = pT +$ higher order terms $\Rightarrow [p]'(0) = p$. Let ω be the normalized differential on $\mathcal{F}$. Then Proposition 5.1.11 says that

$$p\omega(T) = (\omega \circ [p])(T) = F_1(0, [p](T))^{-1} d([p](T)) = (1 + \text{ higher order terms})[p]'(T) dT$$

which implies that

$$[p]'(T) \in pR[[T]] \text{ since } (1 + \text{ higher order terms})^{-1} \in R[[T]].$$

Hence a term $b_i T^i$ is such that $p|i$ or $p|b_i$. □

Theorem 5.1.13. Let R be a discrete valuation ring which is complete with respect to its maximal ideal $\mathcal{M}$ and v be the valuation on R. Assume char $R = 0$ and $p = \text{char } R/\mathcal{M} > 0$ and let $\mathcal{F}/R$ be a formal group. Let z be a non-zero torsion element of $\mathcal{F}(\mathcal{M})$ of order p^n for some positive integer n. Then

$$v(z) \leq \frac{v(p)}{p^n - p^{n-1}}.$$

Proof. Let $\mathcal{H}$ be the cyclic subgroup of $\mathcal{F}(\mathcal{M})$ generated by z. Consider its subgroup

$$\mathcal{H}[p^{n-1}] = \{x \in \mathcal{H} : [p^{n-1}](x) = 0\}$$

and let $\mathcal{H} - \mathcal{H}[p^{n-1}] = \{z_1, z_2, \ldots, z_h\}$. Clearly $z_i = n_i z$ for some n_i satisfying $1 \leq n_i < p^n$ and $(p, n_i) = 1$. Hence $h = |\{i : (i, p^n) = 1\}| = p^n - p^{n-1}$. Since $(p, n_i) = 1$, we must

have $n_i \in R^\times$ so that $v(z_i) = v(z)$ for all i. Write $[p](T) = Tu(T)$ where $u(0) = p$. Define $w(T) = u([p^{n-1}](T))$. Then $w(0) = p$ and $[p^n](T) = [p]([p^{n-1}](T)) = [p^{n-1}](T)w(T)$. We then have $[p^{n-1}](z_i) \neq 0$ and $[p^n](z_i) = [p^{n-1}](z_i)w(z_i) = 0$ so that

$$w(z_i) = 0 \Rightarrow w(T) = (T - z_1)(T - z_2)(T - z_3)\dots(T - z_h)f(T) \text{ where } f(T) \in R[[T]].$$

Setting $T = 0$, we find that $v(p) \geq v(z_1) + v(z_2) + \dots + v(z_h) = hv(z) = (p^n - p^{n-1})v(z)$ which proves the result. □

Now we examine the local group structure of an elliptic curve near the identity.
Consider the Weierstrass equation $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. Consider the change of variables $z = -\frac{x}{y}$ and $w = -\frac{1}{y}$. The fact that z is a uniformizer at O has already been proven. In projective coordinates the transformation is $(X : Y : Z) \mapsto (-X : -Z : Y)$ so that $O \mapsto (0, 0)$ on the following affine piece whose equation is obtained by the change of variables above

$$w = z^3 + (a_1z + a_2z^2)w + (a_3 + a_4z)w^2 + a_6w^3. \tag{5.1.3}$$

Let $f(z, w) = z^3 + (a_1z + a_2z^2)w + (a_3 + a_4z)w^2 + a_6w^3$. We can write w as a formal power series in terms of z by repeated substitution of $w = f(z, w)$ as follows

$$\begin{aligned}
w &= f(z, w) \\
&= z^3 + (a_1z + a_2z^2)w + (a_3 + a_4z)w^2 + a_6w^3 \\
&= z^3 + (a_1z + a_2z^2)(z^3 + (a_1z + a_2z^2)w + (a_3 + a_4z)w^2 + a_6w^3) \\
&\quad + (a_3 + a_4z)(z^3 + (a_1z + a_2z^2)w + (a_3 + a_4z)w^2 + a_6w^3)^2 \\
&\quad + a_6(z^3 + (a_1z + a_2z^2)w + (a_3 + a_4z)w^2 + a_6w^3)^3 + \dots
\end{aligned}$$

Proposition 5.1.14. Indeed the above process converges and gives a formal power series $w(z) \in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6][[z]]$ satisfying $w(z) = f(z, w(z))$.

Proof. Let $R = \mathbb{Z}[a_1, a_2, a_3, a_4, a_6][[z]]$, $\alpha = -1$, $I = \langle z \rangle$, $a = 0$ and $F(w) = f(z, w) - w$. Since $F'(0) = -1 + a_1z + a_2z^2 \in R^\times$, $F(0) = 0$ and $F'(0) \equiv -1 \pmod{I}$, we conclude by the version of Hensel's Lemma in Proposition 5.1.8, that there exists a unique $w(z)$ such that $f(z, w(z)) = w(z)$. □

Making further substitutions, we realize that

$$w(z) = z^3 + a_1z^4 + (a_1^2 + a_2)z^5 + (a_1z^3 + 2a_1a_2 + a_3)z^6 + \dots,$$

and thus in general, we have

$$w(z) = z^3(1 + A_1z + A_2z^2 + A_3z^3 + \dots) \text{ for some } A_1, A_2, \dots \in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6]. \quad (5.1.4)$$

Proposition 5.1.15. There exist power series $i(z), F(z_1, z_2) \in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6][[z]]$ such that $[-1](z, w(z)) = (i(z), w(i(z)))$ and

$$(z_1, w(z_1)) + (z_2, w(z_2)) = (F(z_1, z_2), w(F(z_1, z_2)))$$

where $+$ is the addition on the new curve described by Equation 5.1.3.

Proof. Let z_1 and z_2 be independent indeterminates and set $P_1 = (z_1, w_1)$, $P_2 = (z_2, w_2)$ with $w_1 = w(z_1), w_2 = w(z_2)$. The points lie on the curve given by Equation 5.1.3. Then using $(0, 0)$ as the origin, we can determine the sum $P_3 = P_1 + P_2$. The line through the points has slope

$$\lambda = \lambda(z_1, z_2) = \frac{w(z_2) - w(z_2)}{z_2 - z_1} = \sum_{k=3}^{\infty} A_{k-3}\frac{z_2^k - z_1^k}{z_2 - z_1}$$

which is in $\mathbb{Z}[a_1, a_2, a_3, a_4, a_6][[z]]$. So the straight line has equation $w = \lambda z + \mu$ where $\mu = w_1 - \lambda z_1$, and substituting in Equation 5.1.3 and making rearrangements, we observe that $z_3 \in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6][[z]]$. Let $w_3 = \lambda z_3 + \mu$, then $(z_3, w_3) \in E$. By the uniqueness property we must have $w_3 = w(z_3)$. Clearly $(z_1, w_1) + (z_2, w_2) + (z_3, w_3) = (0, 0)$. For the first part of the claim, set $z_1 = z, z_2 = 0$, so that $i(z) = z_3$ and the second part set $F(z_1, z_2) = i(z_3)$. It turns out that when $z_1 = z_2$ is assumed, one obtains the same results except that calculations are messy, see [8]. □

Computing the first few terms of $F(z_1, z_2)$ gives

$$F(z_1, z_2) = z_1 + z_2 - a_1z_1z_2 - a_2(z_1^2z_2 + z_1z_2^2) - \dots.$$

Proposition 5.1.16. F is a formal group law.

Proof. This is clear from properties of the addition law on E. □

We will use the notation $\hat{E}$ for a formal group associated to an elliptic curve E.

5.2 Reduction

We use the following notation:

K	is a local field with respect to a discrete valuation v.
R	the ring of integers of K.
$R^\times$	the unit group of R.
$\mathcal{M}$	the maximal ideal of R.
π	a local uniformizing parameter of R.
k	the residue field of R.

The Weierstrass equation of E/K, i.e $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ has coefficients in $K = \text{Quot } R$. The transformation $x = u^{-2}x', y = u^{-3}y'$ with $u \in K^\times$ yields a Weierstrass equation with a_i replaced with $u^i a_i$. We can have $u^i a_i \in R$ by choosing u to be divisible by a sufficiently large power of π.

Definition 5.2.1. Let E/K be an elliptic curve defined by a Weierstrass equation (as above). We say that the equation is *minimal* if $a_i \in R$ and $v(\Delta)$ is minimal amongst all curves in the isomorphism class of E. Since $v(\Delta) \in \mathbb{Z}$, such a minimal equation exists.

Proposition 5.2.2. For E/K with Weierstrass equation having integral coefficients, if $v(\Delta) < 12$ or $v(c_4) < 4$ or $v(c_6) < 6$, then the equation is minimal.

Proof. Assume the equation for E is not minimal. Then there is a transformation such that the new discriminant $\Delta' = u^{-12}\Delta$ and $v(\Delta') < v(\Delta)$ for some $u \in K$, $u \neq 0$. It follows that $v(\Delta') = -12v(u) + v(\Delta) < v(\Delta) \Rightarrow u \in R$. Thus $v(\Delta)$ can only be changed by subtracting multiples of 12, so if $v(\Delta) < 0$, that is impossible. On a similar note, recall that $c_4^3 = \Delta j$ and $c_6^2 = \Delta(j - 12^3)$. Using the fact that isomorphic elliptic curves have the same j -invariant, it follows by a similar argument as above that if $v(c_4) < 4$ or $v(c_6) < 6$, then the equation is minimal. □

Proposition 5.2.3. If we begin with any Weierstrass equation for E/K which has coefficients in R, any change of coordinates

$$x = u^2x' + r, \quad y = u^3y' + u^2sx' + t$$

used to come up with a minimal equation, satisfies $u, s, t, r \in R$.

Proof. See [8]. □

Having chosen a minimal Weierstrass equation for E/K, we reduce the coefficients modulo π. We denote $\tilde{a}$, the reduction of a modulo π, and the corresponding reduced curve by $\tilde{E}$. Thus we have $\tilde{E} : y^2 + \tilde{a}_1xy + \tilde{a}_3y = x^3 + \tilde{a}_2x^2 + \tilde{a}_4x + \tilde{a}_6$ with $\tilde{a}_i \in k$. In general for a point $P \in E(K)$, we can find homogeneous coordinates $P = [x_0 : x_1 : x_2]$ with at least one of x_0, x_1, x_2 in $R^\times$. Then the reduced point $\tilde{P} = [\tilde{x}_0 : \tilde{x}_1 : \tilde{x}_2]$ is in $\tilde{E}(k)$. $\tilde{E}/k$ may be singular. Singularity happens when $\Delta \in \mathcal{M}$.
Let $E_1(K) = \{P \in E(K) : \tilde{P} = \tilde{O}\}$, $E_0(K) = \{P \in E(K) : \tilde{P} \in \tilde{E}_{\text{ns}}(k)\}$ and $\tilde{E}_{\text{ns}}(k)$ denote the set of all non-singular points in $E(k)$. Note that $E_{\text{ns}}(k)$ is an abelian group. To see this, for any line passing through two points $P_1, P_2 \in E_{\text{ns}}(k)$, the third point cannot be singular since the multiplicity of a singular point is always at least 2. Hence $E_{\text{ns}}(k)$ is closed under the elliptic curve addition. Since $\pi : \mathbb{P}^2(K) \to \mathbb{P}^2(k)$ takes lines to lines (counting multiplicity), it follows that $\pi : E(K) \to \tilde{E}_{\text{ns}}(k)$ is a homomorphism.

Proposition 5.2.4. We have an exact sequence

$$0 \longrightarrow E_1(K) \xrightarrow{i} E_0(K) \xrightarrow{\pi} \tilde{E}_{\text{ns}}(k) \longrightarrow 0$$

where i is the inclusion map.

Proof. We just need to show that π is surjective. Let $\tilde{P} = (\tilde{\alpha}, \tilde{\beta}) \in \tilde{E}_{\text{ns}}(k)$. Let $\tilde{f} = y^2 + \tilde{a}_1xy + \tilde{a}_3y - x^3 - \tilde{a}_2x^2 - \tilde{a}_4x - \tilde{a}_6$. Then $\tilde{P}$ satisfies

$$\tilde{f}(\tilde{P}) = 0 \text{ and } \frac{\partial \tilde{f}}{\partial x}(\tilde{P}) \neq 0 \text{ or } \frac{\partial \tilde{f}}{\partial y}(\tilde{P}) \neq 0.$$

Assume $\frac{\partial \tilde{f}}{\partial y}(\tilde{P}) \neq 0$. Consider an element $a \in R$ such that $\tilde{a} = \tilde{\alpha}$ and the equation $f(a, y) = 0$. We note that $\tilde{\beta}$ is a root of the polynomial $\tilde{f}(\tilde{a}, y)$ and it is a simple root. So by Hensel's lifting, there exists $b \in R$ such that $b \equiv \tilde{\beta} \pmod{\pi}$ and $f(a, b) = 0$. Clearly $(a, b) \in E_0(K)$. So the reduction map is surjective. On the other hand, the case $\frac{\partial \tilde{f}}{\partial x}(\tilde{P}) \neq 0$ is similar. □

In particular, when $K = \mathbb{Q}_p$, we have

$$0 \longrightarrow E_1(\mathbb{Q}_p) \xrightarrow{i} E_0(\mathbb{Q}_p) \xrightarrow{\pi} \tilde{E}_{\text{ns}}(\mathbb{F}_p) \longrightarrow 0.$$

Proposition 5.2.5. Let E/K be given by a minimal Weierstrass equation, let $\hat{E}/R$ be the formal group associated to E as in Equation 5.1.4. Then the map $\epsilon : \hat{E}(\mathcal{M}) \to E_1(K)$ given by $z \mapsto \left(\frac{z}{w(z)}, -\frac{1}{w(z)}\right), \quad 0 \mapsto O$ is an isomorphism of groups. Recall that $w(z) = z^3(1 + A_1 z + A_2 z^2 + A_3 z^3 + \ldots)$.

Proof. Let $z \in \hat{E}(\mathcal{M})$. Then $w(z)$ converges, and thus $\epsilon(z) \in E(K)$. Now for $w(z) \neq 0$, $\left(\frac{z}{w(z)}, -\frac{1}{w(z)}\right)$ is $[z : -1 : w(z)]$ in homogeneous coordinates. We also have $v(1 + A_1 z + A_2 z^2 + A_3 z^3 + \ldots) = v(1) = 0$ so that $v(w(z)) = 3v(z) \Rightarrow v(w(z)) > 0$ since $v(z) > 0$. That means

$$[z : -1 : w(z)] \equiv [0 : \tilde{1} : 0] = \tilde{O} \pmod{\pi}$$

which implies that $\left(\frac{z}{w(z)}, -\frac{1}{w(z)}\right) \in E_1(K)$. So the map is well defined. It is actually a homomorphism since in constructing the formal group law for $\hat{E}$, the group law for E was used in the zw-plane. We also note that ϵ is injective since $w(z) = 0$ if and only if $z = 0$. Hence $E(\mathcal{M}) \hookrightarrow E_1(K)$.

Let $(x, y) \in E_1(K)$. As $(x, y) = \tilde{O} \pmod{\pi}$, it follows that $v(x) < 0$ or $v(y) < 0$. We claim that $v(x) < 0$ and $v(y) < 0$. To see this, suppose that $v(x) < 0$. If $v(y) \geq 0$, from the Weierstrass equation, we have

$$v(y^2 + a_1 xy + a_3 y) = v(x^3 + a_2 x^2 + a_4 x + a_6) = 3v(x).$$

But

$$\begin{aligned} v(y^2 + a_1 xy + a_3 y) &\geq \min\{v(y^2 + a_3 y), v(a_1 y) + v(x)\} \\ &\geq \min\{v(y^2 + a_3 y), v(x)\} = v(x) \end{aligned}$$

which is a contradiction since $3v(x) < v(x)$.

Assume $v(y) < 0$, and $v(x) > 0$. Then $v(x^3 + a_2 x^2 + a_4 x + a_6) \geq 0$ and

$$v(y^2 + a_1 xy + a_3 y) = \min\{2v(y), v(y) + v(a_1 x + a_3)\} = 2v(y) < 0,$$

a contradiction.

Recall that $v(x^3 + a_2 x^2 + a_4 x + a_6) = 3v(x)$. We will show that $v(y^2 + a_1 xy + a_3 y) = 2v(y)$. Assume $2v(y) \geq v(a_1 xy + a_3 y)$. Then $2v(y) \geq v(y) + v(a_1 x + a_3)$ which implies that

$$\begin{aligned} v(y) &\geq \min\{v(a_1) + v(x), v(a_3)\} \\ &\geq \min\{v(x), v(a_3)\} = v(x), \end{aligned}$$

i.e $v(y) \geq v(x)$. So we have

$$\begin{aligned} v(y^2 + a_1xy + a_3y) &\geq v(a_1xy + a_3y) \\ &\geq \min\{v(a_1) + v(xy), v(a_3) + v(y)\} \\ &\geq v(x) + v(y) \geq 2v(x). \end{aligned}$$

This is a contradiction to the fact that $v(y^2 + a_1xy + a_3y) = 3v(x)$, so we must have $2v(y) < v(a_1xy + a_3y)$ so that $v(y^2 + a_1xy + a_3y) = 2v(y)$. Thus we note that $2v(y) = 3v(x) = -6s$ for some $s \in \mathbb{Z}_{>0}$. It is now easy to see that $v\left(\frac{x}{y}\right) > 0$, so $-\frac{x}{y} \in \mathcal{M}$ which makes the following map

$$\tau : E_1(K) \to \hat{E}(\mathcal{M}), \quad (x, y) \to -\frac{x}{y}, \ O \mapsto 0$$

well defined. This map is a homomorphism of groups since the group law on $\hat{E}(\mathcal{M})$ was computed using the group law on E. The map τ is injective since $\frac{x}{y} = 0 \Rightarrow x = 0 \Rightarrow v(x)$ is not finite. Hence $E_1(K) \hookrightarrow E(\mathcal{M})$. The fact that $\tau^{-1} = \epsilon$ implies that ϵ is an isomorphism. □

For the case of the p-adic field $\mathbb{Q}_p$, we have $E_1(\mathbb{Q}_p) \cong \hat{E}(p\mathbb{Z}_p)$ as groups.

Proposition 5.2.6. Consider E/K and let $m \in \mathbb{Z}$ such that $(m, \text{char } k) = 1$. Then

a. $E_1(K)$ has no non-trivial points of order m.

b. If $\tilde{E}/k$ is non-singular, then $E(K)[m] \hookrightarrow \tilde{E}(k)$.

Proof. a) Use $E_1(K) \cong \hat{E}(\mathcal{M})$ and Proposition 5.1.7.
b) The non-singularity assumption implies that $E_0(K) = E(K)$ and from the exact sequence in Proposition 5.2.4, we have $E(K)/E_1(K) \cong \tilde{E}(k)$ and the result follows using (a). □

Theorem 5.2.7. Consider an elliptic curve $E/\mathbb{Q}_p : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ where $a_i \in \mathbb{Z}_p$. If $p \neq 2$ or $p = 2$ and $2|a_1$, then $E_1(\mathbb{Q}_p) \cong \hat{E}(p\mathbb{Z}_p)$ has no elements of order p.

Proof. Using the substitution $x' = x$ and $y = \frac{a_1}{2}x + y$, we obtain $E' \cong E$ with the equation

$$y^3 + a_1'y = x^3 + a_2'x^2 + a_4'x + a_6'.$$

Note the reason we needed $2|a_1$ if $p = 2$. Maintaining the notation for the original Weierstrass equation, we can assume that $a_1 = 0$. The formal group law is then

$$F(z_1, z_2) = z_1 + z_2 - a_2(z_1^2 z_2 + z_1 z_2^2) - \dots .$$

If $x, y \in p^n\mathbb{Z}_p$, then $x \oplus y = F(x, y) = x + y - a_2(x^2y + xy^2) - \ldots \equiv x + y \bmod p^{3n}\mathbb{Z}_p$. Recall that $[p](x) = F([p-1](x), x) \equiv [p-1](x) + x \bmod p^{3n}\mathbb{Z}_p$. Iterating this several times, we get $[p](x) \equiv px \bmod p^{3n}\mathbb{Z}_p$. So if $x \neq 0$ and $v_p(x) = n$, then $v_p([p](x)) = n + 1 \Rightarrow [p](x) \neq 0$. Thus a non-trivial element of finite order cannot have order p. □

Corollary 5.2.8. With the notation in Theorem 5.2.7, let $a_i \in \mathbb{Z}$ and $2|a_1$. Then $E_1(\mathbb{Q}_p)$ has no non-trivial point of finite order for any p. In particular, if $P \in E(\mathbb{Q})$ is a point of finite order, then $x(P), y(P) \in \mathbb{Z}$.

Proof. Let P have order m. We know that char $\mathbb{F}_p = p$. The assertion is clear for the case when $(m, p) = 1$, see Proposition 5.2.6 (a). Otherwise, $m = p^s r$ with $(r, p) = 1$. We know that $E_1(\mathbb{Q}_p)[p] = \{O\}$. Assume $E_1(\mathbb{Q}_p)[p^s r]$ is non-trivial. Then there exists $P \neq O$ such that $\tilde{P} \in \tilde{O}$ and $p^s rP = O$. Clearly $p^{s-1}rP$ is an element of order p and so $p^{s-1}rP \in E_1(\mathbb{Q}_p)[p]$. We must have $p^{s-1}rP = O$. Repeating this several times, we eventually arrive at $rP = O$ which means that the order of P divides r. Since $(r, p) = 1$, this order is relatively prime to p, the characteristic of the residue field. Applying Proposition 5.2.6 (a) now with $m = r$ we observe that $P = O$, a contradiction. For the particular case, P being a non-trivial point of finite order implies that $v_p(x(P)) \geq 0$ and $v_p(y(P)) \geq 0$ for every prime $p \in \mathbb{Z}$, i.e $x(P), y(P) \in \mathbb{Z}$. □

Remark 5.2.9. If the hypothesis conditions of the preceding proposition hold and that for some prime p, $\tilde{E}/\mathbb{F}_p$ is non-singular. Then from the fact that $E(\mathbb{Q}) \hookrightarrow E(\mathbb{Q}_p)$ and Proposition 5.2.6 (b), we have $E(\mathbb{Q})_{\text{tors}} \hookrightarrow \tilde{E}(\mathbb{F}_p)$. This gives us some information about the torsion subgroup of $E/\mathbb{Q}$. We demonstrate this in the following example.

Example 5.2.10. Consider the elliptic curve $E/\mathbb{Q}_2$ given by

$$y^2 + y = x^3 + 2x^2 + 6x + 1.$$

This elliptic curve has $\Delta = -3^3 13^2$ and $a_1 = 0$. Because 7 and 11 do not divide Δ, $\tilde{E}/\mathbb{F}_7$ and $\tilde{E}/\mathbb{F}_{11}$ are non-singular and

$$\tilde{E}(\mathbb{F}_7) = \{\tilde{O}, (4,1), (4,5)\}$$

$$\tilde{E}(\mathbb{F}_{17}) = \{\tilde{O}, (0,3), (0,7), (3,4), (3,6), (4,0), (4,10), (5,5), (6,2), (6,8), (7,0), (7,10), (9,0), (9,10)\}$$

We have $\#\tilde{E}(\mathbb{F}_7) = 3$ and $\#\tilde{E}(\mathbb{F}_{17}) = 14$, and so it follows that $\#E(\mathbb{Q})_{\text{tors}} = 1$, i.e $E(\mathbb{Q})$ has no non-trivial torsion point. We have $(3905/16, 246243/64) \in E(\mathbb{Q})$ which means that $E(\mathbb{Q})$ has infinitely many points.

Remark 5.2.11. Because $\Delta \neq 0$ is divisible by only finitely many primes, it follows from Remark 5.2.9 that for some p, $E(\mathbb{Q}_p)_{\text{tors}}$ is finite. In particular, $E(\mathbb{Q})_{\text{tors}}$ is finite. Corollary 5.2.8 tells that all points in $E(\mathbb{Q})_{\text{tors}}$ have integer coordinates but does not give us a procedure on how to compute them. We shall prove the so called Nagell-Lutz theorem for certain elliptic curves $E/\mathbb{Q}$. The theorem will give us a constructive approach of computing the torsion subgroup.

We let $f(x) = x^3 + a_2x^2 + a_4x + a_6$ where $a_i \in \mathbb{Z}$ and δ the discriminant of $f(x)$.

Lemma 5.2.12. Let $E/\mathbb{Q}$ be an elliptic curve given by $y^2 = f(x)$. Let $P = (x, y) \in E(\mathbb{Q})$ such that P and $2P$ have integer coordinates. Then either $y = 0$ or $y^2|\delta$.

Proof. Assume that $y \neq 0$. Let $2P = (x', y')$. Using group law, one computes

$$\lambda^2 = 2x + x' + a_2 \quad \text{where} \quad \lambda = \frac{f'(x)}{2y}.$$

The assumption that x, x' and a_2 are integers implies that $\lambda \in \mathbb{Z}$. So $y|f'(x)$. By calculation, we have

$$\begin{aligned}\delta = &((18a_4 - 6a_2^2)x - (4a_2^3 - 15a_2a_4 + 27a_6))f(x) \\ &+ ((2a_2^2 - 6a_2)x^2(2a_2^3 - 7a_2a_4 + 9a_6)x + (a_2^2a_4 + 3a_2a_6 - 4a_4^2))f'(x).\end{aligned}$$

Since $y^2 = f(x)$, we must have $y|\delta$. One can compute that $x' = \left(\frac{f'(x)}{2y}\right)^2 - a_2 - 2x = \frac{f'(x)^2 - 4f(x)(a_2+2x)}{4y^2}$.

Since x' is an integer, we must have $y^2|f'(x)^2-4f(x)(a_2+2x)$, i.e $f(x)|f'(x)^2-4f(x)(a_2+2x)$. Let $r(x)=f'(x)^2-4f(x)(a_2+2x)$. Then we can write δ as $\delta=r(x)g(x)+f(x)h(x)$ for some polynomials $g(x)$ and $h(x)$ in $\mathbb{Z}[x]$, see [7]. Thus, we must have $f(x)|\delta$, i.e $y^2|\delta$. □

Theorem 5.2.13. (Nagell-Lutz) Let $E/\mathbb{Q}$ be an elliptic curve given by

$$y^2=x^3+a_2x^2+a_4x+a_6 \text{ where } a_i\in\mathbb{Z}$$

and δ be the discriminant of the polynomial $x^3+a_2x^2+a_4x+a_6$, i.e

$$\delta=-4a_2^3a_6+a_2^2a_4^2+18a_2a_4a_6-4a_4^3-27a_6^2.$$

Let $P=(x,y)\in E(\mathbb{Q})_{\text{tors}}$. Then

a. $x,y\in\mathbb{Z}$

b. $y=0$ or $y^2|\delta$

Proof. (a) Follows from Corollary 5.2.8 and (b) follows from Lemma 5.2.12 □

Note that as a consequence of Nagell-Lutz theorem, a point with at least a non-integer coordinate cannot be a torsion point. However, the converse of the theorem is false. We provide an example.

Example 5.2.14. For the elliptic curve $E/\mathbb{Q}: y^2=x^3+x^2+7x$, we compute $\delta=-1\cdot 3^3\cdot 7^2$. Possible candidates for the non-zero y-coordinate are enumerated in the following set

$$\{0,\pm1,\pm3,\pm7,\pm21\}.$$

Checking whether there is a corresponding integer value of x in all cases, we compute that

$$E(\mathbb{Q})_{\text{tors}}=\{\tilde{O},(7,21),(1,3),(0,0),(1,-3),(7,-21)\}.$$

By computing the order of each point, we find that $(7,21)$ has order 6. Thus

$$E(\mathbb{Q})_{\text{tors}}\cong\mathbb{Z}/6\mathbb{Z}.$$

Example 5.2.15. The elliptic curve $E/\mathbb{Q}$ given by $y^2 = x^3 + x + 1$, has $\delta = -31$. In this case, we only have $y = 1$ as a candidate for test. The equation $x^3 + x = 0$ yields $x = 0$ which gives a point $(0, 1)$ on E. But $(0, 1) + (0, 1) = (1/4, -9/8)$. Since $(1/4, -9/8)$ is non-torsion, we conclude that $(0, 1)$ is a non-torsion point. Hence $E(\mathbb{Q})_{\text{tors}}$ is the trivial group. In this example, we see that the converse of Nagell-Lutz theorem is not necessarily true.

Example 5.2.16. Let $E/\mathbb{Q}$ be an elliptic curve defined by $y^2 = x^3 - 16x$. Then $\delta = 2^{14}$. We find that the set of possible candidates for the y-coordinate is

$$\{0, \pm 1, \pm 2, \pm 2^2, \pm 2^3, \pm 2^4, \pm 2^5, \pm 2^6, \pm 2^7\}.$$

Testing for each value, we find the following torsion subgroup.

$$\{O, (4, 0), (0, 0), (-4, 0)\}.$$

Furthermore, we observe that every element has order 2. Thus we have

$$E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

The elliptic curves above to which we applied the Nagell-Lutz theorem are of the form $y^2 = x^3 + ax^2 + bx + c$. We will deduce integrality conditions for torsion points for elliptic curves with generalised Weiertrass equations in the following theorem.

Theorem 5.2.17. Let E/K be an elliptic curve given by the equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with $a_i \in R$. Assume char $K = 0$ and $p = \text{char } R > 0$. Let $P \in E(K)$ be a point of order $m \geq 2$. Then $x(P), y(P) \in R$ if m is not a power of p. Otherwise, i.e if $m = p^n$ for some positive integer n, $\pi^{2s}x(P), \pi^{3s}y(P) \in R$ with

$$s = \left\lfloor \frac{v(p)}{p^n - p^{n-1}} \right\rfloor.$$

Proof. For the first part, if $x(P) \in R$, then $y(P) \in R$ so that there is nothing to show. Assume $x(P) < 0$. If the equation for E is not minimal, we can transform the equation

into an equation that is minimal. Denote the coordinates for the minimal equation by (x', y'). By Proposition 5.2.3, we have

$$x = u^2x' + r, \;\; y = u^3y' + u^2sx' + t$$

for some $u, r, s, t \in R$. So we have

$$v(x) \geq \; \min\{v(u^2x'), v(r)\} \geq \; \min\{v(x'), v(r)\} \Rightarrow v(x) \geq v(x')$$

so that $v(x(P)) \geq v(x'(P))$. Similarly, we find that $v(y(P)) \geq v(y'(P))$. Hence we can assume that the equation of E is minimal.

As $v(x(P)) < 0$, we have already seen earlier that $P \in E_1(K)$ and that $3v(x(P)) = 2v(y(P)) = 6r$ for some positive $r \in \mathbb{Z}$. But the group isomorphism $\hat{E}(\mathcal{M}) \cong E_1(K)$ says that $-\frac{x(P)}{y(P)}$ has order m. This contradicts the fact that $\hat{E}(\mathcal{M})$ is a p-group. So we must have $v(x(P)) \geq 0$ and $v(y(P)) \geq 0 \Rightarrow x(P), y(P) \in R$.

For the second part, note that $-\frac{x(P)}{y(P)}$ has order p^n and by Theorem 5.1.13, we have

$$s = v\left(-\frac{x(P)}{y(P)}\right) \leq \frac{v(p)}{p^n - p^{n-1}}.$$

Setting $r = \left\lfloor \frac{v(p)}{p^n - p^{n-1}} \right\rfloor$ yields $v(\pi^{2r}x(P)) = 2r + v(x(P)) \geq 2s + v(x(P)) \Rightarrow \pi^{2r}x(P) \in R$. We also note that $\pi^{3r}y(P) \in R$. □

As a consequence of the theorem, if the coefficients $a_i \in \mathbb{Z}$, i.e $a_i \in \mathbb{Z}_p$ for every prime p and $P \in E(\mathbb{Q})$ is a point of order m which is not a prime power, then $x(P), y(P) \in \mathbb{Z}$. This follows from the fact that we can embed $E(\mathbb{Q})$ in $E(\mathbb{Q}_p)$ for every prime p.

Chapter 6

Bounds on torsion points

The references used in this chapter are [1], [4], [3],[5], [8], [9] and [10].
We survey some known results on torsion subgroups of elliptic curves. We will notice that in some cases, the exact cardinality is not known in general but a bound is. We also look at a result by Breuer [1] in the context of elliptic curves without complex multiplication. Furthermore, we provide several examples that verify the results in certain cases.

6.1 The case of $\mathbb{F}_q$ and $\mathbb{Q}$

We have an exact formula for computing $\#E(\mathbb{F}_q)$ provided the trace of Frobenius is known. We recall from Theorem 3.3.12 that

$$q + 1 - 2\sqrt{q} \leq \#E(\mathbb{F}_q) \leq 2\sqrt{q} + q + 1.$$

Let $I = [q + 1 - 2\sqrt{q}, 2\sqrt{q} + q + 1]$. We table a few cases that verify this bound. This is shown in the table below. For a given elliptic curve E defined over $\mathbb{F}_q$, we compute I as well as the number $\#E(\mathbb{F}_q)$ as shown.
For a number field K, $E(K) \cong E(K)_{\text{tors}} \times \mathbb{Z}^s$ for some non-negative integer s. This is the Modell-Weil Theorem [8]. The number s is called the rank of E. Now we look at the case when $K = \mathbb{Q}$.
We saw ealier that the torsion subgroup $E(\mathbb{Q})_{\text{tors}}$ can be computed in finitely many steps using the Nagell-Lutz Theorem. It is clear that for a prime p that does not divide Δ,

q	E	$\#E(\mathbb{F}_q)$	I
2	$y^2+xy=x^3+x^2+1$	2	[0.175728752538.., 5.828427124746..]
3	$y^2=x^3+2x^2+x+1$	5	[0.5358983848622.., 7.464101615137..]
4	$y^2+y=x^3+\alpha$	1	$[1,9]$
5	$y^2=x^3+x^2+x$	8	[1.527864045000.., 10.47213595499..]
7	$y^2=x^3+6x$	8	[2.708497377870.., 13.29150262212..]
11	$y^2=x^3+9x+6$	10	[5.366750419289.., 18.63324958071..]
13	$y^2=x^3+3x^2+10$	19	[6.788897449072.., 21.21110255092..]
17	$y^2=x^3+11$	18	[9.753788748764.., 26.24621125123..]
19	$y^2=x^3+18x^2+2$	28	[11.28220211291.., 28.71779788708..]
25	$y^2=x^3+4x^2+4x+\alpha+2$	30	$[16,36]$

Table 6.1: Hasse's bound verification

$\#E(\mathbb{Q})_{\text{tors}} \leq \#E(\mathbb{F}_p)$, and so by Hasse's bound, we must have

$$\#E(\mathbb{Q})_{\text{tors}} \leq 2\sqrt{p}+p+1.$$

We say that an elliptic curve E has a good reduction at a prime p if p does not divide Δ (the discriminant of E).

Example 6.1.1. Consider $E/\mathbb{Q}$ defined by the equation $y^2 = x^3 - 25x$. Using the Nagell-Lutz theorem, we obtain

$$E(\mathbb{Q})_{\text{tors}} = \{O, (5,0), (0,0), (-5,0)\}.$$

Note that $E/\mathbb{Q} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ as there is no point of order 4 and every non-trivial point is of order 2. Clearly, $\#E(\mathbb{Q})_{\text{tors}} = 4$. The smallest prime for which E has a good reduction is 3 since $\Delta = 2^6 \cdot 5^6$. Clearly $4 < 2\sqrt{3}+3+1$.

The structure of $E(\mathbb{Q})_{\text{tors}}$ is completely known. This is because of the following theorem due to Mazur, see [8].

Theorem 6.1.2. (Mazur's Theorem) Let E be an elliptic curve defined over $\mathbb{Q}$. Then

$$E(\mathbb{Q})_{\text{tors}} \cong \begin{cases} \mathbb{Z}/m\mathbb{Z} & \text{for } m = 1,2,3,\ldots,10,12 \\ \text{or } \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z} & \text{for } m = 1,2,3,4. \end{cases}$$

The theorem gives us possible subgroups that can occur.

Example 6.1.3. Consider $y^2 = x^3 - 432x + 8208$. We note that

$$E(\mathbb{Q})_{\text{tors}} = \{O, (-12,108), (24,-108), (24,108), (-12,-108)\} \cong \mathbb{Z}/5\mathbb{Z}.$$

Referring to Mazur's Theorem, in this example we have $m = 5$.

Example 6.1.4. For $y^2 = x^3 - 24003x + 1296702$, we obtain

$$E(\mathbb{Q})_{\text{tors}} = \{O, (471, 9720), (147, 972), (111, 0), (147, -972), (471, -9720), (66, 0)$$
$$, (39, 648), (-69, 1620), (-177, 0), (-69, -1620), (39, -648)\}$$

We note that

$$6(471, 9720) = 6(39, 648) = 6(-69, 1620) = O, 3(147, 972) = O$$

and

$$2(111, 0) = 2(66, 0) = 2(-177, 0) = O.$$

Furthermore, by calculation, we observe that every $P \in E(\mathbb{Q})_{\text{tors}}$ is such that $P = i(39, -648) + j(111, 0)$ for some $i, j \in \mathbb{Z}$. Hence

$$E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

so that $m = 3$.

We enumerate a few more cases in the following table as a verification of Mazur's theorem.

E	group structure	m
$y^2 = x^3 - 5x$	$\mathbb{Z}/2\mathbb{Z}$	2
$y^2 = x^3 - 64x$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	1
$y^2 = x^3 - 4x + 1$	$\mathbb{Z}/\mathbb{Z}$	1
$y^2 = x^3 + 4x$	$\mathbb{Z}/4\mathbb{Z}$	4
$y^2 = x^3 + 25$	$\mathbb{Z}/3\mathbb{Z}$	3
$y^2 = x^3 - 1386747x + 36863688$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	4
$y^2 = x^3 - 12987x - 263466$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	2

Table 6.2: Some of the possible groups

6.2 Finitely generated characteristic zero fields

Mazur's result was generalized to a quadratic number field by Kamienny [3], Kenku and Momose [4], and Merel [5] settled the general case. Merel showed that given a number

field of degree at most $d \geq 1$, the cardinality of the torsion subgroup of an elliptic curve defined over the number field is bounded by a constant that depends only on d. There have been developments in trying to come up with bounds as functions of the degree of extension to general fields other than number fields. A result by Breuer [1] expresses an upper bound of the number of L-rational torsion points on a given elliptic curve over a finitely generated field K as a function of the degree $[L : K]$. We discuss this result in the context of elliptic curves without complex multiplication.

Throughout this section, unless otherwise specified, K is a finitely generated characteristic zero field, K^{sep} is the separable closure of K in $\bar{K}$ and L is a finite extension of K. We set $G_K := \text{Gal}(K^{\text{sep}}/K)$.

Definition 6.2.1. Let a be a non-zero element of $\mathbb{Z}$ and E an elliptic curve. The set $E[a]$ is called the a-torsion submodule of E and was defined already. The a-power torsion submodule is given by $E[a^\infty] = \cup_{n\geq 1} E[a^n]$ and $E_{\text{tor}} = \cup_{a\in\mathbb{Z}} E[a]$ is called the full torsion submodule. We also define

$$E_{\text{tor}}(L) := \{x \in E : \sigma(x) = x \ \forall\, \sigma \in \text{Gal}(K^{\text{sep}}/L)\}.$$

Let G_K act on $E[a]$. After fixing a basis for $E[a]$, one gets a Galois representation

$$\rho_a : G_K \to \text{Aut}(E[a]) \cong \text{GL}_2(\mathbb{Z}/a\mathbb{Z}).$$

The index of $\rho_a(G_K)$ is denoted by $I(a)$, i.e

$$I(a) = (\text{GL}_2(\mathbb{Z}/a\mathbb{Z}) : \rho_a(G_K)).$$

Example 6.2.2. Consider an elliptic curve $E : y^2 = x^3 + ax^2 + bx + c$ over $\mathbb{Q}$. It is clear that E is a $\mathbb{Z}$-module. Furthermore, for every $m \neq 0$, we have $E[m] \cong (\mathbb{Z}/m\mathbb{Z})^2$. Consider the field $\mathbb{Q}(x_1, y_1, \ldots, x_n, y_n) = \mathbb{Q}(E[m])$ where we adjoin the coordinates of all finite m-torsion points (x_i, y_i), $i = 1, 2 \ldots, n = m^2 - 1$. Fix a basis P_1, P_2 of $E[m]$. Let $\sigma \in \text{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})$. Then $\sigma([m]P) = [m](\sigma(P))$,i.e the Galois action commutes with the action of $\mathbb{Z}$. For $P \in E[m]$, $\sigma(P)$ is completely determined by specifying $\sigma(P_1)$ and $\sigma(P_2)$. Suppose $\sigma(P_1) = aP_1 + cP_2$ and $\sigma(P_2) = bP_1 + dP_2$. We use the following matrix notation

$$(\sigma(P_1), \sigma(P_2)) = (P_1, P_2) \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Let $\rho_m : \mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ be defined as

$$\rho_m(\sigma) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

A calculation shows that ρ_m is a homomorphism and thus a Galois representation.
We note that the coordinates of m-torsion points are algebraic and can be obtained from polynomials called division polynomials. About division polynomials for torsion points, refer to [10]. For instance, in Example 4.2.8, for $m = 2$, we needed the points (x, y) to satisfy $x^3 + ax^2 + bx + c = 0$. For $m = 3$ in Example 4.2.9, to find 3-torsion points, we needed x to satisfy $3x^4 + 4ax^3 + 6bx^2 + 12cx + 4ac - b^2 = 0$.

Lemma 6.2.3. Let $d \geq 3, t \geq 3$ and $r \geq 1$ be integers. Given that $d \geq B\frac{t^r}{\log\log t}$, it follows that $t \leq B'(d \log\log d)^{1/r}$ for some constant $B' = B'(B, r)$, i.e B' depends on r and the constant B.

Proof. If $d \geq B\frac{t^r}{\log\log t}$, i.e $d \geq (\frac{B}{\log\log t})t^r$, then we can find a constant B_h with $h > 0$ such that $d \geq B_h t^{r-h}$. Here, B_h means that the constant depends on h. Then we have $d/B_h \geq t^{r-h} \Rightarrow \log\log(d/B_h) \geq \log\log(t^{r-h}) = \log(r-h) + \log\log t$, i.e $\log\log(d/B_h) - \log(r-h) \geq \log\log t$. Thus $\log\log t \leq \log\log(d/B_h) \leq B'' \log\log d$ for some constant B''. From the hypothesis condition, we must have $t^r \leq \frac{1}{B} d \log\log t$ so that $t^r \leq \frac{B''}{B} d \log\log d$ and the result follows. □

Lemma 6.2.4. Let K_1 and K_2 be fields. The compositum of the fields K_i's, for $i = 1, 2$ is denoted by K_1K_2. Let K_i/K and L_i/K_i be finite extensions in $\bar{K}$, $i = 1, 2$. Then

$$\frac{[K_1 : K][K_2 : K]}{[K_1K_2 : K]} \leq \frac{[L_1 : K][L_2 : K]}{[L_1L_2 : K]}.$$

Proof. By definition, L_1L_2 is the smallest field containing both L_1 and L_2, and the same applies to K_1K_2. So we must have

$$[L_1 : K_1][L_2 : K_2] \geq \frac{[L_1L_2 : K]}{[K_1K_2 : K]},$$

i.e

$$\frac{[L_1 : K_1][L_2 : K_2]}{[L_1L_2 : K]} \geq \frac{1}{[K_1K_2 : K]}$$

But

$$[L_1 : K_1] = \frac{[L_1 : K]}{[K_1 : K]} \quad \text{and} \quad [L_2 : K_2] = \frac{[L_2 : K]}{[K_2 : K]}$$

so that

$$\frac{[L_1 : K][L_2 : K]}{[K_1 : K][K_2 : K]} \frac{1}{[L_1 L_2 : K]} \geq \frac{1}{[K_1 K_2 : K]},$$

and the result follows. □

Let $T \subset E[a]$ where a is a non-zero integer. We set $\mathrm{Fix}_{\mathrm{Aut}(E[a])}(T) = \{\sigma \in \mathrm{Aut}(E[a]) : \sigma(t) = t \ \forall t \in T\}$ and denote the fixed field of $\rho_a^{-1}(\mathrm{Fix}_{\mathrm{Aut}(E[a])}(T))$ by $K(T)$.

Lemma 6.2.5.

$$[K(T) : K] = \left(\rho_a(G_K) : \rho_a(G_K) \cap \mathrm{Fix}_{\mathrm{Aut}(E[a])}(T)\right).$$

When $T = \{x\}$, we write $K(T) = K(x)$.

Proof. See [1]. □

Let a be a non-zero integer. We define $|a| := |\mathbb{Z}/a\mathbb{Z}|$ and

$$\beta(a) = \prod_{p|a} \left(1 - \frac{1}{p}\right)^{-1}$$

in which the product ranges over all prime factors of a.

Lemma 6.2.6. Let $a \in \mathbb{Z}$ be non-zero. Then $\beta(a) \leq B \log\log|a|$. Furthermore, if $a_n = \prod_{p \leq n} p$ holds, then $\beta(a_n) \geq B' \log\log|a|$ for all $n \in \mathbb{N}$. In either case, B and B' are absolute constants.

Proof. See [1] □

Lemma 6.2.7. Let p be a prime integer and n be an integer greater than or equal to 1. Then we have the exact sequence

$$1 \to 1 + A_2(p\mathbb{Z}/p^n\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}) \to 1$$

where A_2 denotes the additive group of 2×2 matrices.

Proof. Let $A \in 1 + A_2(p\mathbb{Z}/p^n\mathbb{Z})$. Then $\det(A) = 1 + y$ where $y \in p\mathbb{Z}/p^n\mathbb{Z}$. Note that $(\mathbb{Z}/p^n\mathbb{Z})/(p\mathbb{Z}/p^n\mathbb{Z}) \cong \mathbb{Z}/p\mathbb{Z}$, which is a field. Furthermore, any ideal of $\mathbb{Z}/p^n\mathbb{Z}$ is of the form $b\mathbb{Z}/p^n\mathbb{Z}$ where $b\mathbb{Z}$ is an ideal of $\mathbb{Z}$ with $p^n\mathbb{Z} \subseteq b\mathbb{Z}$, i.e $b|p^n$. Thus we have $b\mathbb{Z} = p^k\mathbb{Z}, k = 1, \ldots, n$ and so it follows that $\mathbb{Z}/p^n\mathbb{Z}$ is a local ring with the maximal ideal $p\mathbb{Z}/p^n\mathbb{Z}$. Since $\det(A) \equiv 1 \mod (p\mathbb{Z}/p^n\mathbb{Z})$, i.e $\det(A) \notin p\mathbb{Z}/p^n\mathbb{Z}$ which implies that $\det(A)$ is a unit in $\mathbb{Z}/p^n\mathbb{Z}$. So we have the natural inclusion $1 + A_2(p\mathbb{Z}/p^n\mathbb{Z}) \subset \mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$. We claim that the map $(x_{ij} + p^n\mathbb{Z}) \to (x_{ij} + p\mathbb{Z})$ is a surjective homomorphism from $\mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$ onto $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. This is because given $(x_{ij} + p\mathbb{Z})$ with $\det(x_{ij}) \notin p\mathbb{Z}$, then $\det(x_{ij} + p^n\mathbb{Z}) \notin p\mathbb{Z}/p^n\mathbb{Z}$. The fact that $p\mathbb{Z}/p^n\mathbb{Z}$ is the unique maximal ideal of $\mathbb{Z}/p^n\mathbb{Z}$ implies that $\det(x_{ij} + p^n\mathbb{Z})$ is a unit in $\mathbb{Z}/p^n\mathbb{Z}$. □

Lemma 6.2.8. For a non-zero integer a, we have

$$|\mathrm{GL}_2(\mathbb{Z}/a\mathbb{Z})| = |a|^4 \prod_{p|a} \left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{p^2}\right)$$

where the product ranges over the prime factors of a.

Proof. Without loss of generality, we can assume that $a > 0$. Then $a = p_1^{r_1}p_2^{r_2}\ldots p_m^{r_m}$ for some prime integers $p_1, p_2, \ldots, p_m$. Thus

$$\mathbb{Z}/a\mathbb{Z} \cong \mathbb{Z}/p_1^{r_1}\mathbb{Z} \times \mathbb{Z}/p_2^{r_2}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_m^{r_m}\mathbb{Z}$$

by the Chinese Remainder theorem. So we have

$$(\mathbb{Z}/a\mathbb{Z})^2 \cong (\mathbb{Z}/p_1^{r_1}\mathbb{Z})^2 \times (\mathbb{Z}/p_2^{r_2}\mathbb{Z})^2 \times \ldots \times (\mathbb{Z}/p_m^{r_m}\mathbb{Z})^2$$

which implies that

$$\mathrm{GL}_2(\mathbb{Z}/a\mathbb{Z}) \cong \mathrm{GL}_2(\mathbb{Z}/p_1^{r_1}\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/p_2^{r_2}\mathbb{Z}) \times \ldots \times \mathrm{GL}_2(\mathbb{Z}/p_m^{r_m}\mathbb{Z}).$$

Thus $\mathrm{GL}_2(\mathbb{Z}/a\mathbb{Z})$ is multiplicative in a. It is enough to show the result for $a = p^n$ where p is a prime integer. The ring $\mathbb{Z}/p\mathbb{Z}$ is a finite field containing p elements. In such case, from the theory of automorphism groups of vector spaces over finite fields, we know that

$$\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}) = (p^2 - 1)(p^2 - p).$$

Then from the exact sequence in Lemma 6.2.7, we have

$$\mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})/(1 + A_2(p\mathbb{Z}/p^n\mathbb{Z})) \cong \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$$

so that

$$\begin{aligned}|\mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})| &= |p\mathbb{Z}/p^n\mathbb{Z}|^4|\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})| \\ &= p^{4(n-1)}p^4\left(1-\frac{1}{p}\right)\left(1-\frac{1}{p^2}\right) \\ &= p^{4n}\left(1-\frac{1}{p}\right)\left(1-\frac{1}{p^2}\right).\end{aligned}$$

□

Lemma 6.2.9. Let F and H be subgroups of a finite group G. Then $(F : F \cap H) \leq (G : H)$.

Proof. Define a map $\phi : F \times H \to G$ by $(f, h) \mapsto fh$. Let $f_1h_1 = f_2h_2$. Then $f_2^{-1}f_1 = h_2h_1^{-1} = x \in F \cap H$ so that $f_1 = f_2x$ and $h_1 = x^{-1}h_2$. i.e $(f_1, h_1) = (f_2x, x^{-1}h_2)$. So for a fixed $g \in \phi(F \times H)$, we have

$$|\{t \in F \times H : \phi(t) = g\}| = |F \cap H|.$$

Hence

$$\frac{|F \times H|}{|F \cap H|} = |\phi(F \times H)| \leq |G|$$

which implies that

$$\frac{|F|}{|F \cap H|} \leq \frac{|G|}{|H|}.$$

□

Proposition 6.2.10. Let $x \in E_{\mathrm{tor}}$ have order a. It follows that

$$[K(x) : K] = \frac{1}{\delta}a^2\prod_{p|a}\left(1-\frac{1}{p^2}\right)$$

where $\delta \in [1, I(a)]$.

Proof. Choosing a basis for $E[a]$ such that x is the first basis element, we see that $J \in \mathrm{Fix}_{\mathrm{Aut}(E[a])}(x)$ if and only if $Jx = x$, i.e J is of the form $J = (a_{ij})$, $a_{ij} \in \mathbb{Z}/a\mathbb{Z}$, $1 \leq i, j \leq 2$ with $a_{11} = 1$, $a_{21} = 0$ and $a_{22} \in \mathrm{GL}_1(\mathbb{Z}/a\mathbb{Z})$, i.e a_{22} is a unit in $\mathbb{Z}/a\mathbb{Z}$. Since we can choose $a_{12} \in \mathbb{Z}/a\mathbb{Z}$ arbitrary, we thus have

$$|\mathrm{Fix}_{\mathrm{Aut}(E[a])}(x)| = a|\mathrm{GL}_1(\mathbb{Z}/a\mathbb{Z})|.$$

Using Lemma 6.2.8, we have

$$|\mathrm{Fix}_{\mathrm{Aut}(E[a])}(x)| = a^2 \prod_{p|a} \left(1 - \frac{1}{p}\right)$$

Let $T = \{x\}$ in Lemma 6.2.5. Then

$$\begin{aligned}
[K(x) : K] &= \frac{|\rho_a(G_K)|}{|\rho_a(G_K) \cap \mathrm{Fix}_{\mathrm{Aut}(E[a])}(x)|} \\
&= \frac{|\mathrm{GL}_2(\mathbb{Z}/a\mathbb{Z})|}{I(a)} \cdot \frac{\left(\mathrm{Fix}_{\mathrm{Aut}(E[a])}(x) : \mathrm{Fix}_{\mathrm{Aut}(E[a])}(x) \cap \rho_a(G_K)\right)}{|\mathrm{Fix}_{\mathrm{Aut}(E[a])}(x)|} \\
&= \left(\frac{I(a)}{\left(\mathrm{Fix}_{\mathrm{Aut}(E[a])}(x) : \mathrm{Fix}_{\mathrm{Aut}(E[a])}(x) \cap \rho_a(G_K)\right)}\right)^{-1} \cdot \frac{|\mathrm{GL}_2(\mathbb{Z}/a\mathbb{Z})|}{|\mathrm{Fix}_{\mathrm{Aut}(E[a])}(x)|}
\end{aligned}$$

It is clear that

$$\left(\mathrm{Fix}_{\mathrm{Aut}(E[a])}(x) : \mathrm{Fix}_{\mathrm{Aut}(E[a])}(x) \cap \rho_a(G_K)\right) \geq 1$$

which implies that

$$\frac{I(a)}{\left(\mathrm{Fix}_{\mathrm{Aut}(E[a])}(x) : \mathrm{Fix}_{\mathrm{Aut}(E[a])}(x) \cap \rho_a(G_K)\right)} \leq I(a).$$

On the other hand, setting $F = \mathrm{Fix}_{\mathrm{Aut}(E[a])}(x)$, $H = \rho_a(G_K)$ and $G = \mathrm{GL}_2(\mathbb{Z}/a\mathbb{Z})$ in Lemma 6.2.9 yields the inequality

$$\left(\mathrm{Fix}_{\mathrm{Aut}(E[a])}(x) : \mathrm{Fix}_{\mathrm{Aut}(E[a])}(x) \cap \rho_a(G_K)\right) \leq I(a)$$

so that

$$\frac{I(a)}{\left(\mathrm{Fix}_{\mathrm{Aut}(E[a])}(x) : \mathrm{Fix}_{\mathrm{Aut}(E[a])}(x) \cap \rho_a(G_K)\right)} \geq 1$$

and the result holds by setting $\delta = \frac{I(a)}{\left(\mathrm{Fix}_{\mathrm{Aut}(E[a])}(x) : \mathrm{Fix}_{\mathrm{Aut}(E[a])}(x) \cap \rho_a(G_K)\right)}$ and using Lemma 6.2.8. □

Recall the zeta-function on $\mathbb{Z}$, $\zeta(s) = \prod_p (1 - p^{-s})^{-1}$ where the product ranges over all prime integers.

Proposition 6.2.11. Let a be a non-zero integer and $x_1, x_2 \in E[a]$ be a basis. Then there is a constant C such that

$$\frac{\prod_{i=1}^{2}[K(x_i) : K]}{[K(E[a]) : K]} \leq C\beta(a)$$

and C depends on $I(a)$.

Proof. Let $T = E[a]$ in Lemma 6.2.5. Then $\mathrm{Fix}_{\mathrm{Aut}(E[a])}(E[a]) = \{1\}$ so that

$$[K(E[a]) : K] = |\rho_a(G_K)| = \frac{1}{I(a)}|\mathrm{GL}_2(\mathbb{Z}/a\mathbb{Z})|.$$

Using Lemma 6.2.8 and Proposition 6.2.10, we have

$$\begin{aligned}
\frac{\prod_{i=1}^{2}[K(x_i) : K]}{[K(E[a]) : K]} &= \frac{I(a)\prod_{i=1}^{2}[K(x_i) : K]}{|\mathrm{GL}_2(\mathbb{Z}/a\mathbb{Z})|} \\
&\leq \frac{I(a)\prod_{i=1}^{2}\left(|a|^2\prod_{p|a}\left(1-\frac{1}{p^2}\right)\right)}{|\mathrm{GL}_2(\mathbb{Z}/a\mathbb{Z})|} \\
&= \frac{I(a)|a|^4\prod_{i=1}^{2}\prod_{p|a}\left(1-\frac{1}{p^2}\right)}{|a|^4\prod_{p|a}\left(1-\frac{1}{p}\right)\left(1-\frac{1}{p^2}\right)} \\
&= I(a)\prod_{p|a}\left(1-\frac{1}{p}\right)^{-1}\left(1-\frac{1}{p^2}\right) \\
&\leq I(a)\prod_{p|a}\left(1-\frac{1}{p}\right)^{-1} \\
&= I(a)\beta(a).
\end{aligned}$$

□

Lemma 6.2.12. Let a and b be non-zero integers such that $b|a$. Then $I(b) \leq I(a)$.

Proof. Let $\theta : \mathrm{GL}_2(\mathbb{Z}/a\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/b\mathbb{Z})$ be defined as $(x_{ij}) \mapsto (x_{ij} \mod b)$. Note that θ is well defined since $\det(x_{ij}) \in (\mathbb{Z}/a\mathbb{Z})^\times \Rightarrow \det(x_{ij}) \in (\mathbb{Z}/b\mathbb{Z})^\times$. We also note that $\ker\theta = \{g \in \mathrm{GL}_2(\mathbb{Z}/a\mathbb{Z}) : g \equiv 1 \mod b\}$ where 1 is the identity matrix. Denote by $\tilde{\theta}$ the restriction of θ to $\rho_a(G_K)$. Clearly $\rho_b(G_K) = \tilde{\theta}(\rho_a(G_K))$ and $\ker\tilde{\theta} = \ker\theta \cap \rho_a(G_K)$ which implies that

$$\frac{|\rho_a(G_K)|}{|\ker\theta \cap \rho_a(G_K)|} = |\rho_b(G_K)|.$$

Recall that

$$\begin{aligned}
I(b) &= \frac{|\mathrm{GL}_2(\mathbb{Z}/b\mathbb{Z})|}{|\rho_b(G_K)|} \\
&= \frac{|\mathrm{GL}_2(\mathbb{Z}/b\mathbb{Z})| \cdot |\ker\theta \cap \rho_a(G_K)|}{|\rho_a(G_K)|} \\
&= \frac{|\mathrm{GL}_2(\mathbb{Z}/a\mathbb{Z})| \cdot |\ker\theta \cap \rho_a(G_K)|}{|\rho_a(G_K)||\ker\theta|}
\end{aligned}$$

and

$$I(a) = \frac{|\mathrm{GL}_2(\mathbb{Z}/a\mathbb{Z})|}{|\rho_a(G_K)|}.$$

Calculation shows that

$$\frac{I(b)}{I(a)} = \frac{|\ker\theta \cap \rho_a(G_K)|}{|\ker\theta|} \leq 1 \Rightarrow I(b) \leq I(a).$$

□

Theorem 6.2.13. Let E be an elliptic curve over K without complex multiplication. Then

a. There is a constant C depending on E and K so that for any finite extension L/K,

$$|E_{\mathrm{tors}}(L)| \leq C([L:K]\log\log[L:K])^{1/2}.$$

a. Consider a prime integer p. There is a constant C depending on E, K and p such that for every finite extension L/K,

$$|E[p^\infty](L)| \leq C[L:K]^{1/2}.$$

Proof. Recall that G_K acts on $E[a]$, giving a Galois representation

$$\rho_a : G_K \to \mathrm{Aut}(E[a]) \cong \mathrm{GL}_2(\mathbb{Z}/a\mathbb{Z}).$$

The index $I(a) = (\mathrm{GL}_2(\mathbb{Z}/a\mathbb{Z}) : \rho_a(G_K))$ is bounded independently of a. This is due to Serre [6].

Let $T = E_{\mathrm{tors}}(L)$ and a be the smallest positive integer for which $T \subset E[a]$. Choose a basis x_1, x_2 of $E[a]$ with the property that T is generated by y_i's with $y_i \in \langle x_i\rangle$ and y_i is of order a_i where $i = 1, 2$. Thus $K(T) = \prod_{i=1}^2 K(y_i)$. By Lemma 6.2.4, Proposition 6.2.11 and Lemma 6.2.6, we have

$$\begin{aligned}\frac{\prod_{i=1}^2[K(y_i):K]}{[K(T):K]} &\leq \frac{\prod_{i=1}^2[K(x_i):K]}{[K(E[a]):K]} \\ &\leq B_1\beta(a) \leq B_2\log\log a\end{aligned}$$

where B_2 does not depend on T. Using Proposition 6.2.10, we have

$$\begin{aligned}
[K(T):K] &\geq \frac{\prod_{i=1}^{2}[K(y_i):K]}{B_2 \log\log a} \\
&\geq \frac{1}{(B_2 \log\log a)\prod_{i=1}^{2}\delta_i} \prod_{i=1}^{2}\prod_{p|a_i}\left(1-\frac{1}{p^2}\right) a_1^2 a_2^2 \quad \text{where} \quad 1 \leq \delta_i \leq I(a_i) \\
&\geq \frac{1}{(B_2 \log\log a)\prod_{i=1}^{2} I(a_i)} \prod_{i=1}^{2}\prod_{p|a_i}\left(1-\frac{1}{p^2}\right) a_1^2 a_2^2 \\
&\geq \frac{1}{(B_2 \log\log a)\prod_{i=1}^{2} I(a_i)} \cdot \prod_{i=1}^{2}\left(\frac{1}{\prod_p \left(1-\frac{1}{p^2}\right)^{-1}}\right) \cdot a_1^2 a_2^2 \\
&\geq \frac{1}{I(a)^2\zeta(2)^2} \cdot \frac{a_1^2 a_2^2}{B_2 \log\log a} \quad \text{since} \quad I(a_i) \leq I(a) \text{ for all } i. \\
&\geq B_3 \frac{|T|^2}{\log\log|T|}
\end{aligned}$$

where B_3 is a constant that neither depends on T nor $I(a)$.

Now (a) follows from Lemma 6.2.3 by setting $t = |T|$, $r = 2$ and $d = [K(T) : K]$. Furthermore, if $T = E[p^\infty]$, then $a = p^n$ for some $n \in \mathbb{N}$. But $\beta(p^n) = (1-p^{-1})^{-1}$ which depends only on p and so $\log\log|T|$ is a constant that depends on p. Thus part (b) follows. □

The theorem gives an upper bound on the cardinality of the torsion subgroup with coordinates in a specified extension.

Chapter 7

Applications of elliptic curves

The references used in this chapter are [7] and [10].
Elliptic curves have several applications. Some of the known applications occur in cryptography and we will discuss them in this chapter.

7.1 Diffie-Hellman Key Exchange

Given an elliptic curve E defined over a finite field. Let P be a non-trivial point and $Q \in \langle P \rangle$. The elliptic curve discrete logarithm problem (ECDLP) seeks to find an integer x such that $xP = Q$. Generally, it is difficult to efficiently solve this problem if the sought integer x is very large. Cryptosystems built based on the ECDLP are secure as long as one does not find such an x very easily. One such cryptosystem is the Diffie-Helmann key exchange in which two people exchange a private key that will be used for later communication. We will call the two parties communicating Alice and Bob. The stages in the key exchange are highlighted below.

The shared key K_s is computed to be the first coordinate of $n_b C_a$. If Alice and Bob are to communicate safely using their newly shared private key, then they have to make sure that n_a and n_b are kept secret. Thus an 'enemy' who presumably knows C_a and C_b will have to solve the ECDLP $mP = C_a$ or $wP = C_b$ and extract the key from mC_b or wC_a, respectively. To see why this is true, note that $mP = n_a P$ so that $m \equiv n_a + kr$ for some integer r, and $k = |\langle P \rangle|$. Hence $mC_b = (n_a + kr)C_b = n_a n_b P$ from which K_s can

Diffie-Hellman key exchange
1. *Public parameter creation*
A trusted party publishes a large prime p, an elliptic curve E defined over $\mathbb{F}_p$ and a point $P \in E(\mathbb{F}_p)$.
2. *Private computations*
Alice chooses a secret integer n_a and computes $C_a = n_a P$. Bob chooses a secret integer n_b and computes $C_b = n_b P$.
3. *Value exchange*
Bob sends to Alice C_b and Alice sends to Bob C_a.
4. *Key computation*
Alice computes $n_a C_b = n_a n_b P$ and Bob computes $n_b C_a = n_b n_a P$.

be extracted. The other case is similar.

There are various tools for solving ECDLP in certain cases. But in general, it still remains a difficult problem.

Example 7.1.1. Suppose that the trusted authority publishes $E : y^2 = x^3 + 1000x + 16$, $p = 1000117$ and $P = (0, 4)$. Assume that Alice and Bob choose their secret integers $n_a = 189$ and $n_b = 157$, respectively. Then $C_a = (586177, 754447)$ and $C_b = (205963, 547583)$. Thus $n_a C_b = 189(205963, 547583) = 157(586177, 754447) = (872536, 465976)$. So their shared key $K_s = 872536$ which they can use for communication.

7.2 Integer factorisation

The RSA cryptosystem, which is based on the difficulty to factorise a composite integer, is unsafe if a highly efficient algorithm can be found for integer factorization. A number of methods have been developed to factor integers. One of them uses elliptic curves. The method is called Lenstra's method. We will present the idea behind this method and implement it in SAGE with some modification.

For simplicity, assume we want to factor a large composite integer n which is a product of two primes p and q.

We consider an elliptic curve E mod n. Let P be a point on this curve. In trying to compute $2P$, we first find the gradient of the tangent line at P. Let d be the denominator of the gradient we are computing. If d^{-1} mod n exists, then we proceed. Otherwise, $\gcd(d, n) \neq 1$ and so we have found a factor of n. If we are lucky, this factor may be

non-trivial. The algorithm is provided below. For specific technical details, refer to [10].

Elliptic curve factorisation

1. Choose an elliptic curve E mod n at random and a point P on E.

2. Choose an integer B and try to compute $(B!)P$.

3. If (2) fails at some point, then we have found a factor of n.

4. If (2) succeeds, then increase B or use a different elliptic curve and repeat the process.

Definition 7.2.1. Let n and B be a positive integers. Consider the prime factorisation $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$. Then n is called B-smooth if $p_i \leq B$ for all i.

The reason for $B!$ in the above algorithm is that if we choose several random elliptic curves E, probably one of them will have a point P whose order is B-smooth and thus $(B!)P = O$. So, at this stage we may find our factors. Note that if n is B-smooth, then all its distinct prime factors divide $B!$.
In practice B is chosen to be around 10^8.

Example 7.2.2. Suppose we would like to factor 35. Consider the curve $y^2 = x^3 - 20x + 21$. An easy calculation shows that $P = (15, -4)$ is a point on E. Let us try $B = 20$. We have the following computations.
The gradient, λ, at P is $\frac{3(15)^2-20}{-8} = \frac{655}{27}$. Thus $d = 27$ and $d^{-1} \equiv 13 \mod 35$ so that $\lambda = 8515 = 10$. Now $2P = (x, y)$ is such that $x = 10^2 - 30 = 0$ and $y = -10(0 - 15) + 4 = 14$. So $2P = (0, 14)$. We now compute $3P = 2P + P$. Here, $\lambda = \frac{14+4}{-15} = \frac{7}{15}$. We note that 15^{-1} does not exist mod 35. So we have found a factor! This factor is $\gcd(15, 35) = 5$ and so the other factor is just $\frac{35}{5} = 7$.

The example above shows the existence of situations where B may not play its role. However, we cannot tell in advance whether setting B will be relevant or not.

We therefore propose an implementation of the algorithm in which B is not taken into consideration. The implementation is based on SAGE syntax as shown in the Appendix, item 3. Here is the description of the program.

We assume the input n is a positive integer made up of two distinct primes (though we can as well consider the arbitrary case). The program creates an elliptic curve curve of the form $y^2 + ax + a^2$ where $a \in \mathbb{Z}/n\mathbb{Z}$. So we work on this elliptic curve mod n. Then the program creates a point $P = (0, a)$ on the curve. It computes $2P, 3P, 4P, \ldots$. In the process of computing the points, at each stage of computing the gradient, it computes the greatest common divisor (gcd) of the denominator and n. If the gcd is equal to n, then it creates a new curve and a new point on this curve. If the gcd is equal to 1, it proceeds computing the gradient. If none of the above cases occurs, then a non-trivial factor has been found, and the program computes a factor of n by calculating the gcd of n and the denominator of the gradient at that stage. The program stops only when a non-trivial factor has been found.

Chapter 8

Conclusion

Elliptic curves are indeed an interesting class of algebraic curves. From the definition of their group law, we notice the interplay between geometry and algebra. Such a curve can be realised as a non-singular cubic equation with at least a point on it. This makes the study of elliptic curves better as we are reduced to the case of cubic equations. When defined over various fields, results for elliptic curves vary. For instance, when the base field is finite, we have seen that exact formulae for the size of points with specified coordinates can be derived. On the other hand, if the base field is not finite, you can have infinite or finite size and the structure of the torsion subgroup can be complicated in general.
We have noted that complex elliptic curves are the same as tori. This helps us understand the structure of the m-torsion subgroups and such a structure can be made more precise. A proof of the Nagell-Lutz theorem using formal groups has been presented as opposed to using detailed explicit computations that involve transforming the origin to a finite point and working with the new equation. Of course that required deriving the formal group associated to an elliptic curve. The Nagell-Lutz theorem is one of the important theorems if the torsion subgroup for elliptic curves defined over $\mathbb{Q}$ is sought. This is because it gives an algorithm for computing torsion points in finitely many steps. A survey of some general results on torsion points has been made and several examples given in order to verify the results. Of great importance is the fact that elliptic curves have several practical applications. An area of cryptography called elliptic curve cryptography is devoted to studying such applications. In this thesis, we only presented two amongst the many applications which are known. Thus one can factor integers as well as do a

key exchange. We implemented Lenstra's elliptic curve factorisation without taking into account the smoothness property. This consideration was done in a hope that we may still be able to factorize integers.

Appendix A

Computer Algebra System

Built-in SAGE commands used to aid our computations. Its not our work.

1. Elliptic curves over number fields

```
#input a1,a2,a3,a4,a6
E=EllipticCurve([a1,a2,a3,a4,a6]);
# elliptic curve y^2 +a1*x + a3*xy =x^3 + a2*x^2 + a4*x + a6
G = E.torsion_subgroup();
#the torsion subgroup of E
len(G);
# size of G
Z =[E(t) for t in G];
#Z is the set of points in G
```

2. Elliptic curves over finite fields

```
#input p,i,a1,a2,a3,a4,a6
F.<a> = GF(p^i, 't');
# Finite field of size p^i and t is a root of minimal polynomial
E=EllipticCurve([a1,a2,a3,a4,a6]);
# elliptic curve y^2 +a1*x + a3*xy =x^3 + a2*x^2 + a4*x + a6
#Elliptic curve defined over F_{p^i}
E.points()
```

```
#List of points on E
```

The following code is our work based on SAGE syntax.

3. Integer factorisation code

```
def ecm_factor(n): # n = pq, p and q distict primes
    R = Integers(10000000000000000000)
    factor = n + 1
    while(factor >= n):
        a = int(R.random_element())
        b = a*a % n
        while(4*a^3 + 27*b^2 % n == 0):
            a = int(R.random_element())
            b = a*a
        P = [0,int(a)]
        x1 = P[0]
        x2 = P[0]
        y1 = P[1]
        y2 = P[1]
        s = 2*y1 % n
        see = gcd(int(s),n)
        while gcd(see,n)==1:
            if x1 == x2:
                red1 = 3*x1*x1 + int(a) % n
                red2 = 2*y1 % n
                r = gcd(int(red2),n)
                if r == 1:
                    c = inverse_mod(int(2*y1),n)
                    grad = red1*c % n
                    x3 = grad*grad - 2*x1 % n
                    y3 = grad*(x1 - x3) - y1 % n
                    x1 = x2
                    x2 = x3
```

```
                    y1 = y2
                    y2 = y3
                else:
                    see = r
            else:
                red1 = y2 - y1 % n
                red2 = x2 - x1 % n
                r = gcd(int(red2),n)
                if r == 1:
                    c = inverse_mod(int(x2 - x1),n)
                    grad = red1*c % n
                    x3 = grad*grad - 2*x1 % n
                    y3 = grad*(x1 - x3) - y1 % n
                    x1 = x2
                    x2 = x3
                    y1 = y2
                    y2 = y3
                else:
                    see = r
        factor = see
    return factor
ecm_factor(1000036000099)
> 1000033
```

List of References

[1] F. Breuer. Torsion bounds for elliptic curves and drinfeld modules. *J. Number Theory*, 130:1241–1250, 2010.

[2] R. Hartshone. *Basic Algebraic Geometry 1.* Springer-Verlag, 1994.

[3] S. Kamienny. Torsion points on elliptic curves. *Bull. Amer. Math. Soc.*, 23:371–373, 1990.

[4] M. Kenku and F. Momose. Torsion points on elliptic curves defined over quadratic fields. *Nagoya Math. J.*, 109:125–149, 1988.

[5] L. Merel. Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Invent. Math*, 124(1–3):437–449, 1996.

[6] J. P. Serre. Propriétés galoisiennes des points d'ordre finides courbes elliptiques. *Invent. Math*, 15(no. 4):259 – 331, 1972.

[7] J. Silverman and J. Tate. *Rational Points on Elliptic Curves.* Springer-Verlag, 1994.

[8] J. H. Silverman. *The Arithmetic of Elliptic Curves.* Springer, 2nd edition, 2000.

[9] S. Susanne and G. Host. *Elliptic Curves: A computational Approach.* Walter de Gruyter, 2003.

[10] L. Washington. *Elliptic Curves: Number Theory and Cryptography.* Chapman and Hall, 2008.